PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10

Disusun Oleh:

N a m a : Adetya Putra Dewanto

NIM : 13523025

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2018

HALAMAN PENGESAHAN DOSEN PEMBIMBING

PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10

TUGAS AKHIR

Disusun Oleh:

N a m a : Adetya Putra Dewanto

NIM : 13523025

Yogyakarta, 9 September 2018

Pembimbing 1,

(Mukhammad Andri Setiawan , S.T., M.Sc., Ph.D.)

Pembimbing 2,

(Fietyata Yudha S.Kom., M.Kom)

HALAMAN PENGESAHAN DOSEN PENGUJI

PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Informatika
di Fakultas Teknologi Industri Universitas Islam Indonesia
Yogyakarta, 3 Oktober 2018

Tim Penguji

Dr. Mukhammad A Setiawan, S.T., M.Sc. _____

Anggota 1

Almed Hamzah, S.T., M.Eng. _____

Anggota 2

Ahmad Fathan Hidayatullah, S.T., M.Sc. _____

Mengetahui,
Ketua Program Studi Teknik Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Adetya Putra Dewanto

NIM : 13523029

Tugas akhir dengan judul:

PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 1 Nopember 2018

(Adetya Putra Dewanto)

HALAMAN PERSEMBAHAN

Alhamdulillahi Robbil ‘Alamin. Segala puji dan syukur atas kehadirat Allah Subhana Wa Ta’ala yang telah memberikan rahmat, ridho, dan karunia-Nya serta nikmat yang tiada tara kepada saya. Shalawat serta salam kepada Nabi Muhammad Shallallahu ‘Alaihi Wasallam, sebagai pembawa risalah Allah terakhir dan penyempurna seluruh risalah-Nya yang telah membawa umatnya dari zaman yang gelap gulita ke zaman yang terang benderang. Tugas akhir ini kupersembahkan untuk semua orang yang aku cintai. Terutama teruntuk kepada Ibu tersayang yang tidak pernah lelah memberikan kasih sayang, bimbingan akhlak, dan doa dari kecil hingga sekarang. Kepada Ayah tercinta yang selalu memberikan kasih sayang, nasehat menghadapi kehidupan, pentingnya kerja keras dan doa. Kepada sahabat-sahabatku, terima kasih atas segala kebersamaan, bantuan, dukungan, pengalaman, nasehat, dan doa yang telah diberikan.

HALAMAN MOTO

"If you are searching for that person who will change your life, take a look in the Mirro"

(Sandeep Maheshwari)

"Yesterday is history, Tomorrow is a mystery, But today is a Gift"

(Bil keane)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan mengucap Alhamdulillah, puji dan syukur atas kehadirat Allah Subhana Wa Ta'ala yang telah memberikan berkat rahmat dan hidayah-Nya, sehingga tugas akhir yang berjudul "**Penetration Testing Pada Domain Uii.ac.id Menggunakan OWASP 10**" dapat diselesaikan dengan baik. Shalawat serta salam tidak lupa senantiasa dilimpahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam, yang telah membawa kita dari zaman jahiliyah menuju ke zaman terang benderang.

Laporan tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata-1 (S1) di Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia. Selain itu, tugas akhir ini juga sebagai sarana untuk menerapkan ilmu dan teori yang telah didapatkan selama menjalani masa studi di jurusan Teknik Informatika Universitas Islam Indonesia.

Akhirnya, dengan segala kerendahan hati izinkanlah penulis untuk menyampaikan rasa terimakasih dan penghargaan yang setinggi-tingginya atas motivasi, bantuan, bimbingan, dan doa. Penulis menyampaikan rasa dan penghargaan tersebut kepada:

1. Kedua orang tua saya yang tidak pernah memberikan do'a, dukungan dan motivasi sehingga penulis dapat menyelesaikan laporan tugas akhir ini

2. Bapak Hendrik, S.T., M.Eng, selaku Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

3. Bapak Mukhammad Andri Setiawan , S.T., M.Sc., Ph.D. selaku Dosen Pembimbing 1 tugas akhir yang telah memberikan masukan, arahan, serta dorongan sehingga penelitian ini dapat terlaksana sehingga tugas akhir ini dapat di selesaikan.

4. Bapak Fietyata Yudha S.Kom., M.Kom selaku Dosen Pembimbing 2 tugas akhir yang telah memberikan ide, masukan, dan bimbingan mengenai cara-cara melakukan penelitian ini, serta arahan dalam pembuatan laporan tugas akhir dan *report* hasil penelitian.

5. Yolandita Ganis Kumala yang tidak pernah bosan memberikan motivasi dan dukungan kepada penulis dalam proses mengerjakan tugas akhir ini

6. Kurniawan Bayu Fitriyansah dan Wahyu Widyaningrum yang selalu membantu dan memberikan banyak saran dan masukan terhadap proses penelitian ini.

7. Sahabat-sahabat terbaik saya yang tidak dapat saya sebutkan satu persatu terimakasih banyak.

8. Teman-teman informatika angkatan 2013 terima kasih atas pengalaman kuliah yang tidak terlupakan.

9. Kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung, semoga Allah SWT menjadikannya amal baik yang senantiasa mendapatkan balasan dan kebaikan berlipat ganda.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 1 Nopember 2018

(Adetya Putra Dewanto)

SARI

Keamanan adalah salah satu aspek penting dalam segala hal. Perkembangan teknologi yang begitu pesat juga berpengaruh terhadap cara individu, organisasi dan pelaku bisnis dalam melakukan proses penyampaian informasi. Di zaman yang berkembang ini informasi menjadi suatu hal yang sangat berharga Universitas Islam Indonesia adalah salah satu organisasi perguruan tinggi yang memanfaatkan kemajuan teknologi yaitu *web* dalam menyampaikan informasi kepada pihak luar dan menghubungkan *civitas academica* yang ada guna memudahkan dalam penyampaian informasi. Seiring dengan kemajuan teknologi pentingnya keamanan terhadap suatu jaringan menjadi hal utama karena mencegah serangan dari orang luar yang tidak bertanggung jawab yang dapat merugikan proses bisnis yang sedang berjalan. Untuk mengetahui seberapa rentangkah suatu jaringan *web* terhadap serangan dari luar perlu dilakukan proses *penetration testing (pentest)* dimana seorang penguji menyimulasikan dirinya seperti pihak luar yang berusaha masuk kedalam jaringan.

Di sini penulis menggunakan metode OWASP10 tahun 2013. Metode ini dipilih karena selalu dilakukan pembaruhan terhadap informasi yang berisi 10 serangan terhadap *web* yang sering ditemukan. Di sini penulis juga menemukan beberapa kendala dalam melakukan proses *scanning* terhadap 10 *web* target yang memiliki domain uii.ac.id dikarenakan banyaknya target yang harus di uji sehingga penulis melakukan pengembangan terhadap aplikasi yang dimiliki OWASPZap dimana aplikasi ini dibuat menjadi otomatis sehingga dapat mempermudah proses *scanning* yang memiliki jumlah taget yang cukup banyak.

Semoga hasil dari proses *pentest* dapat membantu pengelola *web* yang memiliki domain uii.ac.id untuk dapat segera melakukan pencegahan dan pengamanan terhadap *web* yang mereka kelola sehingga dapat mengurangi resiko serangan tidak bertanggung jawab dari luar yang dapat merugikan Universitas Islam Indonesia dan diharapkan pengembangan aplikasi otomatisasi OWASPZap ini juga dapat membantu *admin web* dalam melakukan proses *pentest* di kemudian hari

Kata kunci: Informasi, web, *Penetration testing*, OWASP10, *Scanning*, OWASPZap

GLOSARIUM

Backdoors	Sebuah software atau mekanisme yang digunakan untuk mengakses sistem atau software maupun sebuah jaringan.
Crawling	Sebuah teknik yang digunakan untuk memindai halaman pada suatu website.
Debian	Sistem operasi berbasis linux.
Denial of Service	Salah satu jenis serangan yang bertujuan untuk mencegah user yang berwenang dalam melakukan akses.
DNS	Suatu sistem yang berguna untuk menyimpan informasi host atau domain dari suatu jaringan.
Email	Surat elektronik.
Firewall	Sistem keamanan jaringan yang berguna melindungi komputer dari serangan.
Flowchart	Gambaran alur dari suatu proses.
Host	Sistem antar server yang saling terhubung secara langsung.
IP Address	Identitas dari semua perangkat komputer dan alat komputer dengan menggunakan indentitas tertentu.
Javascript	Bahasa yang digunakan untuk membuat program.
Kali Linux	Sebuah sistem operasi yang ada karena pengembangan sistem operasi Debian.
Library	Kumpulan pustakan yang siap dipakai dalam pengembangan aplikasi.
MAC Address	Sebuah identitas unik yang diberikan produsen kepada suatu perangkat komputer yang terhubung ke jaringan.
Penetration Testing	Sebuah metode yang dilakukan untuk menguji keamanan dari sebuah sistem dimana penguji melakukan simulasi penyerangan terhadap sistem.
Port	Sebuah mekanisme dalam komputer yang bertujukan untuk mendukung beberapa sesi koneksi.
Python	Suatu bahasa pemrograman.
Scanning	Proses pemindaian sebuah sistem.
Server	Sistem komputer yang menyediakan jenis layanan tertentu pada sebuah jaringan.

Software	Perangkat lunak yang berfungsi untuk mendukung kinerja perangkat keras pada komputer.
Trojan horse	Suatu program yang menjadikan program kita dapat diakses oleh orang lain tanpa ijin kita.
URL	Rangkaian karakter yang digunakan untuk menunjukkan sebuat alamat situs tertentu.
Virus	Sebuah program komputer yang dapat menggandakan atau menyali programnya sendiri dan menyebar dengan cara menyalin dirinya ke dalam suatu dokumen atau program lain.
Vulnerability	Suatu kelemahan pada sistem komputer yang dapat diakses oleh pihak yang tidak berwenang.
Web	Situs
Worm	Sebuah jenis virus komputer yang dapat menduplikasi dirinya, namun tidak dapat menginfeksi program komputer, tetapi dapat membuat kinerja komputer menjadi lambat.

DAFTAR ISI

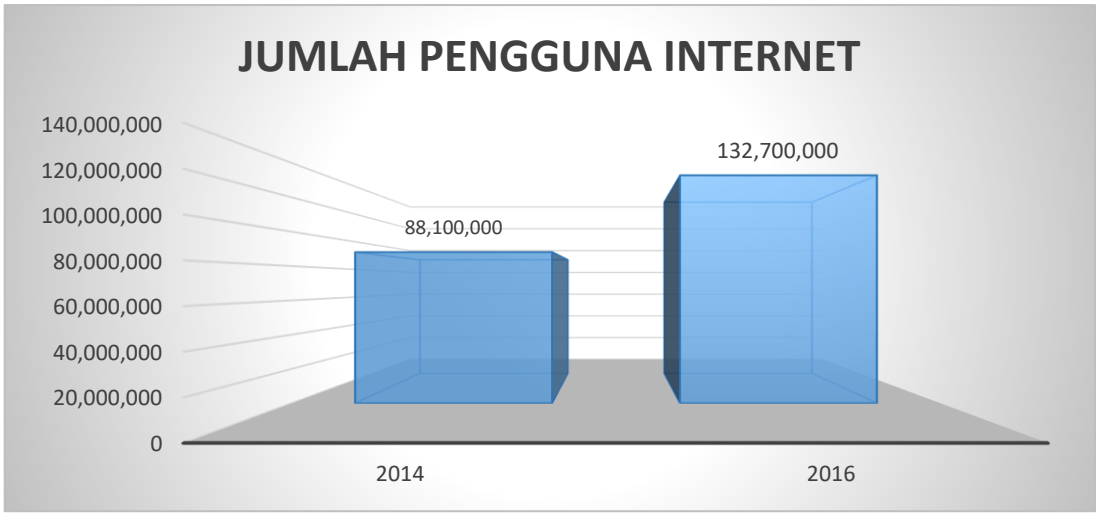
DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

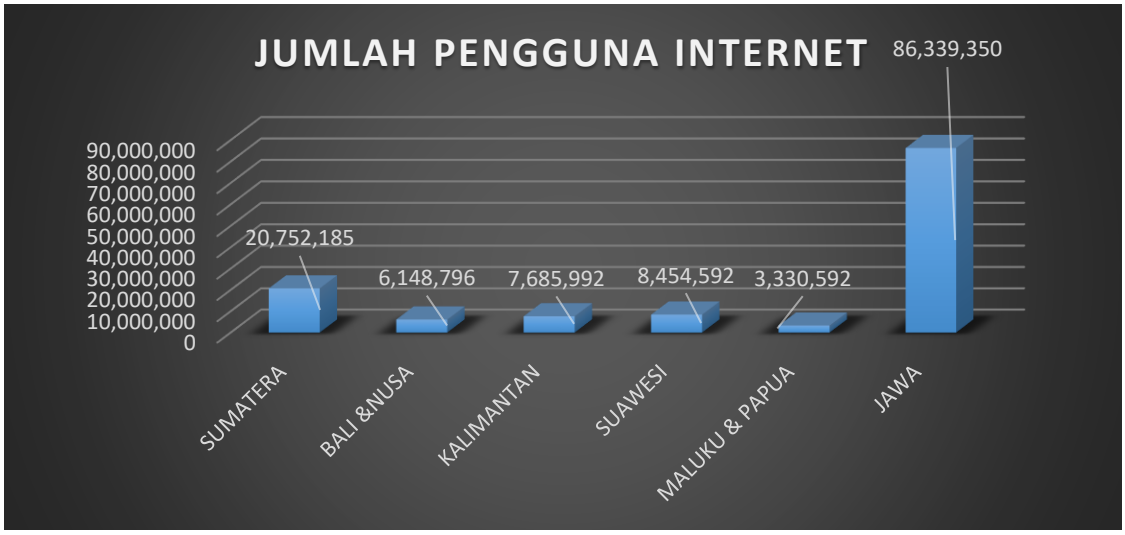
1.1 Latar Belakang

Perkembangan dan evolusi dalam dunia komputer, internet dan teknologi *web* telah begitu pesatnya berkembang sehingga masuk dalam segala lini kehidupan masyarakat kini masyarakat bergantung pada layanan jaringan komputer melebihi masa sebelumnya. Hal ini dapat dilihat dengan semakin banyaknya pengguna media sosial dan layanan internet saat ini.



Gambar 1.1 Jumlah pengguna internet menurut APJII pada tahun 2016

Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia(APJII) pada tahun 2016 seperti yang terlihat pada Gambar 1.1 menunjukan jumlah pengguna Internet di Indonesia tahun 2016 adalah 132,7 juta user dari total jumlah penduduk Indonesia sebesar 256,2 juta Jika dibandingkan penggunaan internet Indonesia pada tahun 2014 sebesar 88,1 juta user, maka terjadi kenaikan sebesar 44,6 juta dalam waktu 2 tahun (2014 – 2016) dan masih didominasi pulau Jawa sebagai pengguna internet terbanyak di Indonesia seperti yang terlihat pada Gambar 1.2 di bawah (Isparmo, 2016). Pengguna internet di Indonesia diprediksi akan terus meningkat setiap tahun.



Gambar 1. 2 Jumlah pengguna internet pada tahun 2016

Dengan semakin bertambahnya pengguna layanan internet maka semakin banyak informasi yang dapat diperoleh dari internet. Informasi sendiri menjadi hal penting di era digital ini baik untuk organisasi, bisnis maupun individu. Semakin banyak individu memberikan informasi tentang mereka di internet membuat semakin menipisnya privasi yang dimiliki belakangan ini banyak individu yang mulai sadar dengan bagaimana informasi yang mereka berikan dimanfaatkan dan semakin banyak pula organisasi yang mulai memperhatikan resiko keamanan informasi yang dapat memberikan dampak buruk dan kerugian materil terhadap proses bisnis, citra terhadap organisasi, kepercayaan pelanggan serta mempengaruhi hubungan dengan pelanggan atau mitra bisnis mereka (Herfiedhantya, 2014).

Universitas Islam Indonesia (UII) sebagai salah satu lembaga pendidikan perguruan tinggi terkemuka di Indonesia memanfaatkan jaringan internet yaitu *web* sebagai media dalam menyampaikan informasi kepada pihak luar dan menghubungkan civitas-civitas yang ada guna memudahkan dalam penyampaian informasi. Pertukaran informasi yang terjadi dalam jaringan internet dapat berupa informasi penting atau pribadi yang hak aksesnya hanya dapat dilakukan oleh orang-orang tertentu (Herfiedhantya, 2014). Namun tidak dipungkiri lagi tidak hanya pihak yang memiliki akses saja yang dapat mengakses informasi tersebut namun mungkin ada pihak-pihak lain yang tidak bertanggung jawab dapat mengaksesnya dan menyalahgunakan informasi yang ada yang menyebabkan kerugian bagi organisasi. Salah satu aturan dasar dalam menentukan keamanan suatu jaringan ada 3 yaitu Confidentiality(kerahasiaan) menjaga kerhasiaan infomarsi dari orang-orang yang tidak berhak, Integrity(integritas) menjaga perubahan informasi dari orang yang tidak berhak dan Availability(ketersediaan) menjaga agar

informasi selalu ada untuk diakses atau disingkat sebagai CIA TRIAD. Jika 3 faktor dasar dalam keamanan jaringan itu tidak dapat terpenuhi maka suatu jaringan dapat dikategorikan tidak aman dan rawan tersusupi oleh pihak yang tidak bertanggung jawab (Handisonj, 2013). Dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan analisis terhadap sistem dan jaringan yang terdapat pada UII dari persepektif luar atau jaringan publik. Penelitian ini berfokus pada pengumpulan informasi dan pengujian sistem yang ada dengan metode *penetration testing* (*pentest*) berdasarkan pada metode *Open Web Application Security Project Top 10* (*OWASP 10*) tahun 2013.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan di atas maka rumusan masalah yang ditetapkan:

a. Bagaimana menguji keamanan dalam domain dan subdomain yang dapat merugikan proses bisnis di lingkungan Universitas Islam Indonesia.
b. Bagaimana mengembangkan aplikasi untuk melakukan pengujian terhadap studi kasus yang ada di Universitas Islam Indonesia.
c. Bagaimana melakukan pengujian terhadap aplikasi yang telah dikembangkan.

1.3 Batasan Masalah

Untuk memfokuskan masalah yang ada, maka diperlukan sebuah batasan-batasan agar bisa terfokus dengan masalah yang ada oleh sebab itu batasan masalah dalam kasus ini sebagai berikut:

a. *Web* yang akan diuji adalah 10 *web* yang terdiri dari 6 fakultas, 2 direktorat dan 2 badan yang menggunakan domain uii.ac.id.
b. Pengujian dilakukan dengan minimal 3 *tools* pada tiap tahap.
c. *Penetration testing* ini mengacu pada OWASP10 tahun 2013.

1.4 Tujuan Penelitian

Adapun tujuan yang diharapakan tercapai dalam melakukan penelitian pengujian celah keamanan ini adalah:

a. Menguji keamanan dari *web* yang berdomain uii.ac.id terhadap serangan dari luar oleh orang yang tidak bertanggung jawab yang dapat merugikan Universitas Islam Indonesia.
b. Mengembangkan aplikasi guna mempermudah melakukan pengujian celah keamanan terhadap serangan dari luar oleh orang yang tidak bertanggung jawab
c. Melakukan pengujian terhadap aplikasi yang telah dikembangkan.
d. Membuat sebuah hasil *pentest* ke dalam sebuah laporan yang dapat dimengerti semua orang.

1.5 Manfaat Penelitian

Manfaat yang diharapkan didapatkan dari penelitian yang dilakukan ini adalah sebagai berikut:

a. Bagi Peneliti:
    1. Dapat mengimplementasikan ilmu pengetahuan yang selama ini diperoleh di perkuliahan.
    2. Mengimplementasikan dan menambah pengetahuan mengenai Bahasa pemrograman *python.*
    3. Mendapatkan pembelajaran baru tentang metode OWASP.
b. Bagi UII:
    1. Mengetahui seberapa rentang *web* Universitas Islam Indonesia terhadap serangan tidak bertanggung jawab dari luar.
    2. Mengetahui celah keamanan dari *web* Universitas Islam Indonesia sehingga dapat dilakukan tindakan penanggulangan sejak dini.
c. Bagi Masyarakat:
    1. Mengembangkan aplikasi yang dapat mempermudah dalam melakukan pengujian celah keamanan pada *web.*
    2. Membatu administrator dalam melakukan pengujian pada *web.*

1.6 Metodologi Penelitian

Metodologi penelitian ini dilakukan agar dalam proses pengujian yang dilakukan dapat lebih terarah, sesuai rencana dan mencapai tujuan yang diharapkan. Adapun metodologi yang diterapkan dalam pembuatan tugas akhir ini adalah sebagai berikut:

a. Pendaftaran alamat IP

Pendaftaran alamat *IP* dilakukan sebagai syarat utama melakukan *penetrasting testing* terhadap domain uii.ac.id agar kita diberikan akses oleh admin dalam hal ini BSI sebagai lembaga pengelola domain uii.ac.id. Di sini penulis mendaftarkan alamat *IP* 103.56.205.230.

b. Footprinting

Tahap awal dalam melakukan penguasaan suatu sistem yaitu dengan cara mengumpulkan segala bentuk informasi mengenai *web* berdomain uii.ac.id yang akan dilakukan *pentest*.

c. Scanning

Setelah mendapatkan informasi mengenai *web* target, proses selanjutnya adalah melakukan *scanning* yaitu proses dimana mencari *port* atau celah keamanan lain pada *web* yang dapat disusupi.

d. Uji penetration

Melakukan pengujian pada *web* berdomain uii.ac.id menggunakan metode OWASP 10.

e. Pembuatan laporan hasil pengujian

Proses penjabaran dan penjelasan hasil dari pengujian yang telah dilakukan menggunakan metode OWASP 10 disertakan solusi menurut metode pengujian.

1.7 Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh mengenai masalah yang akan dibahas dalam penulisan laporan tugas akhir ini, maka sistematika laporan ini dibagi menjadi 5 bab. Adapun penjabarannya sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan laporan *penetration testing* pada *domain* uii.ac.id menggunakan metode OWASP10.

BAB II LANDASAN TEORI

Bab ini membahas tentang gambaran umum tentang teori yang diterapkan dalam pengujian *penetration testing*, menggunakan OWASP 10. Selain itu dalam bab ini juga terdapat penjelasan tentang metode dan *tools* yang digunakan untuk melakukan *penetration testing*.

BAB III METODOLOGI

Bab ini membahas tentang metode yang dilakukan dalam penelitian. Metode tersebut adalah pengumpulan data, analisis kebutuhan serta perancangan pembangunan sistem dan termasuk didalamnya perancangan pengujian yang dilakukan secara sistematis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang langkah-langkah proses pengujian yang dilakukan dan hasil yang didapatkan dari proses pengujian yang dilakukan terhadap beberapa target yang ditentukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi penutup yang meliputi kesimpulan-kesimpulan dari hasil pengujian yang telah dilakukan sebelumnya yang berupa hasil analisis pengujian yang telah dilakukan dan terdapat saran-saran dari hasil pengujian.

BAB II
LANDASAN TEORI

2.1 Kajian Penelitian

Menurut penelitian Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan *Web Server* (Dirgahayu, et.all, 2015) untuk mengamankan *web server* dari serangan *hacker* maka sebaiknya para pemilik *web server* melakukan *self test* terhadap *server* mereka sendiri. Melalui *self test* ini, para pemilik *web server* akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode *self test* ini adalah *penetration test*. Metode ini sama dengan aktivitas *hacking* namun dilakukan secara legal.

Dalam penelitian lain yang dilakukan oleh Zainal Ali Abidin yang berjudul *penetration testing* Menggunakan Metode OWASP (*Open Web Application Security Project*) disebutkan bahwa OWASP dapat digunakan sebagai acuan dalam melakukan pengujian pada suatu sistem lebih sepesifiknya untuk *web application* (Abidin, 2015) dengan demikian OWASP bisa dijadikan sebagai dasar dalam pengujian keamanan terhadap *web* application. Dalam penelitian tersebut target yang diserang adalah *web* SIMSON (Manejemen Skripsi Online) milik Universitas Islam Indonesia. Beberapa penelitian terdahulu lainya dapat dilihat pada .

Tabel 2. 1 Skripsi di Universitas Islam Indonesia dengan judul *penetration testing*

Judul	**Penulis**	**Target**	**Tools**
Penerapan Metode ISSAF dan OWASP versi 4 untuk Uji Kerentanan Web Server	Dr. Raden Teduh Dirgahayu, ST., M.Sc. , Yudi Prayudi S.Si.,M.Kom.,Adi Fajaryanto	IKIP PGRI Madiun	Whois, SSL Scan, Zenmap, Acunetix, Low Orbit Ion Cannon, Havij, Armitage, PHP Rootkits, WebScrap, Brutus, Mozilla Firefox, Wfuzz, Dirb, Zed Attack Proxy, OWASP CSRF Tester
Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)	Mohmmad Muhsin, Adi Fajaryanto	Fakultas Teknik Universitas Muhammadiyah Ponorogo	WebScrab,Brutus,Mozilla Firefox,WFuzz,Dirb,Zed Attack,Proxy, OWASP CSRF Tester
Penerapan Owasp Versi 4 Untuk Uji Kerentanan Web Server (Studi Kasus Ejurnal Server Kampus X Madiun)	Adi Fajaryanto Cobantoro	*Web server* Kampus X Madiun	WebScrab,Brutus,Dirb,WFuzz,Zed Attack Proxy, OWASP CSRF Tester

Judul	Penulis	Target	Tools
Web Application Vulnerability Assessment Used Owasp Application Security Verification Standard (Asvs) For Ugm Websites	Tashia Indah Nastiti	*Website* UGM	Browser, Zed Proxy Attack, Foundstone Sitedigger 3.0, Wappalyzer
Penetration Testing Menggunakan Metode Owasp (Open Web Application Security Project)	Ali Zainal Abidin	Sistem Informasi Manajemen Skripsi Online (SIMSOn) Universitas Islam Indonesia	Sql Injection, Ettercap, Wireshark, Browser

2.2 Dasar Teori

2.2.1 Keamanan Informasi

Keamanan informasi sendiri memiliki pengertian yaitu bagaimana kita dapat mencegah penipuan atau, paling tidak mendeteksi adanya penipuan pada sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Berdasarkan ISO/IEC 17799:2005 yang menjelaskan tentang *information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis Jadi dapat disimpulkan bahwa keamanan informasi adalah mencegah dan mendeteksi tindakan yang berupa akses yang tidak sah, pencurian informasi, perubahan program atau kerusakan fisik terhadap sistem informasi yang dapat menimbulkan kehilangan dan kerugian terhadap proses bisnis yang ada.

Menurut Whitman dalam bukunya yang berjudul Principles of Incident Response and Disaster Recovery (Whitman, July 2007), ada beberapa faktor atau ancaman ancaman dalam keamanan sistem informasi yang antara lain:

a. Kesalahan manusia (*Acts of human error or failure*): ancaman karena kesalahan manusia dimana kejadian tersebut bukan disengaja atau tanpa maksud jahat.
b. Hak Atas Kekayaan Intelektual atau yang biyasa disingkat HAKI (*Compromises to intellectual property* (*IP*)): ancaman dari pelanggaran dalam penggunaan HAKI seperti hak cipta, rahasia dagang, merek dagang, hak Paten. Pelanggaran HAKI yang paling umum adalah pembajakan perangkat lunak.

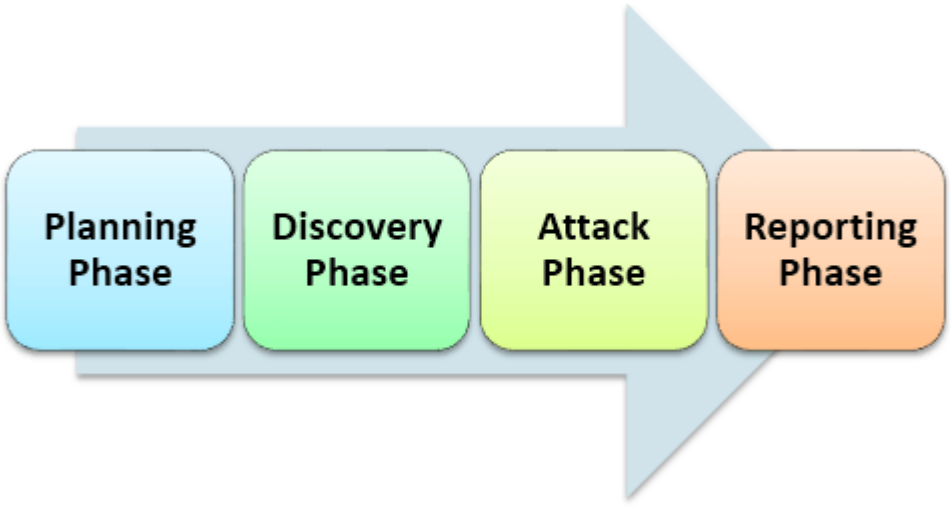
c. Pelanggaran yang disengaja (*Deliberate acts of trespass*): mengakses secara tidak sah ke informasi yang bersifat rahasia dan pribadi. Contohnya seorang hacker menggunakan perangkat lunak untuk mendapatkan akses ke informasi secara ilegal.
d. Tindakan untuk tujuan pemerasan: menuntut kompensasi untuk mengembalikan rahasia informasi yang diperoleh oleh penyerang.
e. Tindakan disengaja untuk sabotase atau vandalisme: Upaya untuk menghancurkan aset atau merusak citra organisasi.
f. Tindakan pencurian yang disengaja: mengambil barang orang lain secara ilegal.
g. Serangan dengan perangkat lunak: perangkat lunak yang berbahaya yang dirancang untuk merusak, menghancurkan, atau menolak layanan ke sistem, termasuk *virus, worm, trojan horse, backdoors, serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS).*
h. Kejadian alam: Tak terduga dan sering tidak dapat diramalkan, termasuk kebakaran, banjir, gempa bumi, petir, badai, letusan gunung berapi.
i. Penyimpangan dalam kualitas pelayanan, oleh penyedia layanan. Produk atau jasa terhenti atau tidak dapat berjalan sebagai mana mestinya seperti listrik, air, bandwidth jaringan, dll.
j. Kerusakan atau kesalahan teknis dari peralatan: Cacat bawaan peralatan yang menyebabkan sistem bekerja tidak sesuai dengan diharapkan, menyebabkan layanan tidak dapat diberikan dengan baik atau kurangnya ketersediaan.
k. Kesalahan dan kegagalan *Software*: Termasuk *bug* dan kondisi tertentu yang belum teruji. Mungkin termasuk cara pintas (*shortcut*) yang sengaja dibuat oleh programmer untuk alasan tertentu tetapi lupa untuk di hapus.
l. Teknik dan peralatan yang telah usang: infrastruktur yang sudah ketinggalan zaman menyebabkan sistem tidak dapat diandalkan dan tidak dapat dipercaya.

Oleh sebab itu untuk mengurangi resiko-resiko yang ada terhadap keamanan suatu informasi dan untuk menjaga ekosistem proses bisnis tetap berjalan sebagaimana mestinya agar tidak menimbulkan kerugian terhadap individu, perusahaan atau organisasi salah satunya perlu adanya pengujian terhadap suatu sistem atau *website* untuk mencari celah keamanan yang terdapat dalam sistem atau *website* tersebut untuk segera dapat dilakukan pencegahan lebih

dini terhadap serangan dari orang yang tidak bertanggung jawab yang dapat menimbulkan kerugian.

2.2.2 Penetration Testing

Penetration Testing adalah sebuah metode pengujian terhadap sebuah sistem atau jaringan komputer yang bertujuan untuk mengevaluasi keamanan sistem atau jaringan komputer tersebut. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*) terhadap suatu sistem atau jaringan guna menemukan celah keamanan yang disebabkan oleh kelemahan dari suatu sistem, konfigurasi yang tidak benar atau kelemahan operasional dalam proses teknis. Laporan hasil dari sebuah *Penetration Testing* akan memberikan masukan terhadap pemelik sistem tentang celah keamanan terhadap sistem mereka yang dapat digunakan sebagai bahan evaluasi dari sistem keamanan komputer yang sedang berjalan guna melakukan penambalan kebocoran celah yang terdapat dalam sistem mereka sehingga dapat segera dilakukan tindakan pencegahaan lebih dini. Proses penetration dapat dilihat pada Gambar 2. 1 di bawah ini.



Gambar 2. 1 *Penetration testing* proses (learn-penetration-testing, n.d.)

2.2.3 Black Box Testing

Black box testing adalah dimana penguji sebagai orang luar yang sama sekali tidak memahami dan memiliki informasi tentang sistem atau jaringan yang akan diuji sehingga penguji harus mencari segala informasi yang berkaitan dengan sistem tersebut untuk dilakukan analisis dan menentukan metode-metode gunak melakukan attack.

2.2.4 White Box Testing

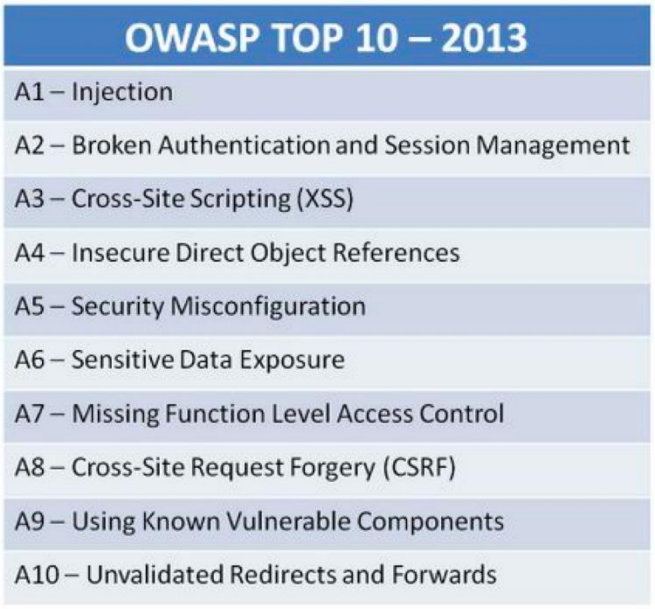
White box testing adalah kebalikan dari *black box testing* dimana penguji telah mengetahui informasi dari sistem atau jaringan yang akan diuji sehingga dapat langsung menentukan metode *attack* yang akan digunakan.

2.3 Open Web Application Security Project (OWASP)

OWASP (*Open Web Application Security Project*) adalah komunitas terbuka yang mendedikasikan untuk membuat sebuah organisasi yang bertujuan untuk mengembangkan, membeli, dan memelihara aplikasi yang terpercaya. Di OWASP pengunjung akan menemukan semua gratis dan terbuka. Seluruh *tools*, dokumen, forum, dan cabang OWASP bebas dan terbuka bagi semua orang yang tertarik memperbaiki aplikasi keamanan. OWASP mendukung pendekatan keamanan aplikasi sebagai masalah perseorangan, proses, dan masalah teknologi karena pendekatan paling efektif terhadap keamanan aplikasi membutuhkan perbaikan diseluruh area. OWASP adalah jenis organisasi baru yang bebas dari tekanan komersial sehingga memungkinkan untuk memberikan informasi terkait keamanan aplikasi yang tidak bias, praktis, dan efektif biaya. OWASP tidak terafiliasi dengan perusahaan teknologi manapun, meskipun OWASP mendukung penggunaan teknologi keamanan komersial. Serupa dengan banyak proyek *software open-source*, OWASP menghasilkan beragam jenis materi dengan cara kolaborasi dan terbuka. Yayasan OWASP merupakan lembaga non-profit yang memastikan kesuksesan jangka panjang proyek. Hampir semua yang terasosiasi dengan OWASP adalah sukarelawan (OWASP, 2011).

2.3.1 OWASP TOP 10

OWASP Top 10 atau yang biasa disebut OWASP10 adalah sebuah daftar yang dirilis oleh komunitas OWASP yang berisikan 10 daftar teratas celah keamanan yang dapat mengancam keamanan suatu *website* daftar ini terus berkembang dan berubah-ubah mengikuti perkembangan teknologi *website* yang terus berkembang. OWASP Top 10 pertama kali dirilis tahun 2003 lalu update minor pada tahun 2004 dan 2007 dan 2010 (OWASP, 2011). OWASP Top 10 sendiri dibuat dengan tujuan untuk meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi beberapa risiko celah keamanan yang sering dihadapi atau ditemui dalam banyak kasus seperti pada Gambar 2. 2.



Gambar 2. 2 OWASP Top 10 tahun 2013

Gambar 2.2. di atas adalah contoh OWASP10 yang dirilis oleh organisasi OWASP yang berisikan 10 celah keamanan yang sering ditemukan pada tahun 2013.

2.4 Scanning Tools

Scanning adalah tahapan di mana penyerang mengumpulkan segala informasi yang berhubungan dengan jaringan korban secara lebih spesifik. *Scanning* juga dapat diartikan sebagai bentuk pendeteksian sistem yang masih hidup dan dapat diakses melalui internet dan apa saja *service* yang ditawarkan. Tahap ini merupakan resiko tinggi, jika penyerang dapat menemukan kelemahan dari sebuah sistem, maka penyerang dapat mengeksploitasi jaringan tersebut. Terdapat banyak cara dan *tools* dalam melakukan proses *scanning* dapat dilakukan secara manual atau otomatis menggunakan *tools* yang banyak bersebaran yang dapat memudahkan penyerang dalam melakukan *scanning*. Beberapa contoh *tools* yang dapat digunakan antara lain The Harvester, Nmap, dan Masscan sebagaimana yang akan dijelaskan lebih detail setelah ini.

2.4.1 The Harvester

The Harvester merupakan salah satu *tools* yang ada di Kali Linux *tools* ini berguna sebagai mesin pencari yang mengumpulkan data berupa *Subdomain, Email, Host, Employee,*

Port dan Banner yang bersumber dari segala sumber publik antara lain: *search engines, PGP key servers and shodan computer database* (Harvester, 2014). Theharvester merupakan *tools* yang diciptakan untuk membantu *penertration tester* pada tahap awal dalam melakukan sebuah pengujian untuk mengumpulkan jejak dari *web* target. *Tools* ini sangat efektif dan sederhana dalam melakukan pengumpulan informasi.

2.4.2 Nmap

Network Mapper (Nmap) merupakan sebuah *tools open source* untuk eksplorasi dan audit keamanan jaringan. Yang dirancang untuk memeriksa jaringan besar secara cepat, selain itu Nmap dapat pula bekerja terhadap *host* tunggal. Nmap menggunakan paket *IP raw* dalam cara yang canggih untuk menentukan *host* mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal *upgrade* layanan, dan melakukan *monitoring uptime host* atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Hal penting di antara informasi itu adalah "tabel *port*". Tabel tersebut berisi daftar angka *port* dan protokol, nama layanan, dan status. Statusnya adalah terbuka (*open*), difilter (*filtered*), tertutup *(closed*), atau tidak difilter (*unfiltered*). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada *port* tersebut. Difilter berarti bahwa terdapat sebuah *firewall, filter,* atau penghalang pada jaringan yang mem*blokir port* sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Aplikasi nmap juga dapat memberikan informasi lebih lanjut tentang target, termasuk nama reverse DNS, prakiraan sistem operasi, jenis device, dan alamat MAC (Nmap, n.d.).

2.4.3 Masscan

Masscan adalah sebuah *tools* yang berfungsi sebagai internet *port* scanner *tools* ini memiliki keunggulan dibanding aplikasi *scanner port* lainya yaitu lebih cepat dalam melakukan *scanning port* (Masscan, 2017). *Tools* ini dapat memiliki kecepatan mengirimkan 100 packet/second pada mode bawaan dan dapat melakukan 25juta packet/second pada mode cepat.

2.4.4 Web Analisys Scanning

Web analisys scanning adalah tahap dimana seorang penyerang melakukan analisis mendalam terhadap *web* target yang akan diserang (*attack*). Terdapat beberapa cara dalam melakukan *web analisys scanning* antara lain dengan cara manual menggunakan *browser* atau dengan menggunakan *tools vulnerability scanner* yang banyak bersebaran. Beberapa contoh *tools vulnerability scanner* antara lain WPScan dan OWASPZap yang akan dijelaskan lebih detail setelah ini.

WPScan

WPScan merupakan salah satu *tools vulnerability scanner* yang digunakan untuk melihat dan mendeteksi kelamahan pada *web* yang bertipe WordPress (Wpscan, 2014). Celah keamanan yang biyasanya terdapat dalam *web* yang bertipe WordPress biyasanya celah keamanan ditemukan dalam *plugin* atau *theme* yang digunakan oleh user pada *web* WordPress mereka. Fungsi WPScan Antara lain:

a. List Plugin
b. List Theme
c. Brute Force Weak Password dan Username (Hanya berlaku pada beberapa user saja)
d. Listing Direktori
e. Melihat kemungkinan vulnerabilities.

OWASPZap

OWASPZap adalah sebuah *tools vulnerabilities scanner* yang dibuat oleh organisasi OWASP *tools* in adalah suatu proyek dari OWASP yang paling aktif karena terus dikembangkan *tools* ini bersifat *opensource* sehingga siapa saja juga bisa mengembangkan *tools* ini. Fitur yang ada dalam OWASPZap antara lain *Intercepting Proxy,Active and Passive Scanners, spider scan, report Generation, Brute Force(using OWASP dirbuster code), Fuzzing(using fuzzdb & OWASP JBrosfuzz), Extensibility,Auto tagging,Port scanner, Parameter analysis, Smart card support, Session comparison, invoke external apps, Api +headless mode, Dynamis SSL Certificates, Anti CSRF token handling* (Owaspzap, 2016). Dengan banyaknya fitur yang terdapat dalam OWASPZap sehingga memudahkan dalam melakukan scanner terhadap suatu *web* selain itu OWASPZap sangat mudah digunakan sehingga memudahkan pemula dalam melakukan *scanning* terhadap *web*.

BAB III
METODE PENELITIAN

3.1 Metode Penelitian

Dalam melakukan penelitian *pentest* terhadap *web* yang ber-subdomain uii.ac.id ini terdapat beberapa tahap dalam pengumpulan data. Tahapan yang dilakukan dalam pengumpulan data ini terdapat beberapa sumber antara lain melalui literatur seperti jurnal, buku, paper ilmiah, tugas akhir atau dari media digital seperti internet. Selain dari itu informasi juga didapatkan melalui hasil analisis pada infrastruktur jaringan dan sistem UII dan melakukan diskusi dengan pihak pengelola jaringan UII dan ahli dalam bidang keamanan informasi atau uji *pentest*.

3.2 Alat Kebutuhan Penelitian

Alat yang digunakan dalam melakukan penelitian ini terdiri dari perangkat keras dan perangkat lunak. Perangkat keras yang digunakan adalah laptop sedangkan perangkat lunak yang digunakan adalah Kali Linux 2.0 dan Python 2.7. Kali Linux adalah salah satu linux yang berbasis menggunakan Debian yang banyak memiliki fitur dan *tools* yang tepat dalam melakukan pengujian *pentest*. Sedangakan Python adalah salah satu bahasa pemrograman *interpretatif multiguna* yaitu bahasa pemrograman yang lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks. Contoh spesifikasi laptop dan sepesifikasi minimum yang dibutuhkan seperti pada Tabel 3. 1.

Tabel 3. 1 Spesifikasi perangkat penelitian.

Komponen	**Spesifikasi Minimum**	**Spesifikasi yang digunakan**
Processor	Pentium 4 atau procesor AMD64	Intel® Core™ i7-4700HQ Processor (2.4 GHz, Cache 6MB) Max Turbo Frequency:3.4 GHz
RAM	512 MB	8
Storage Memory	10GB	1TB
VGA	128MB	NVIDIA® GeForce® GT 745M 2GB

3.2.1 Alur Penelitian

Dalam melakukan penelitian *penetration testing* pada domain uii.ac.id menggunakan metode OWASP10 memiliki beberapa tahapan seperti yang dapat dilihat pada diagram alur yang terdapat pada Gambar 3. 1.

Gambar 3. 1 Diagram alur *penetration testing* pada domain uii.ac.id

Tahapan awal dilakukan identifikasi masalah baik dari informasi yang diperoleh dari berbagai sumber atau dengan pihak yang mengelola jaringan UII. Identifikasi masalah juga dilakukan berdasarkan berbagai sumber lain yang antara lain seperti Tugas akhir skripsi atau tesis yang serupa dengan penelitian ini dan informasi informasi lain yang mendukung.

Tahap selanjutnya setelah mengidentifikasi masalah adalah dengan melakukan studi literatur yang berhubungan dengan konsep keamanan informasi dan uji *pentest* dan jaringan. Studi literatur dilakukan dengan cara mencari buku, skripsi, penelitian ilmiah dan berbagai

sumber informasi yang terdapat di internet guna mendapatkan teori yang cocok dengan penelitian.

Selanjutnya adalah tahap menentukan metode pengujian. Di tahap ini dilakukan diskusi dengan dosen pembimbing berdasrkan studi literatur yang telah dilakukan untuk mencari metode pengujian yang tepat. Kemudian setelah didapatkan metode yang cocok dengan penelitian akan dilakukan tahap pengujian pada target yang telah ditentukan.

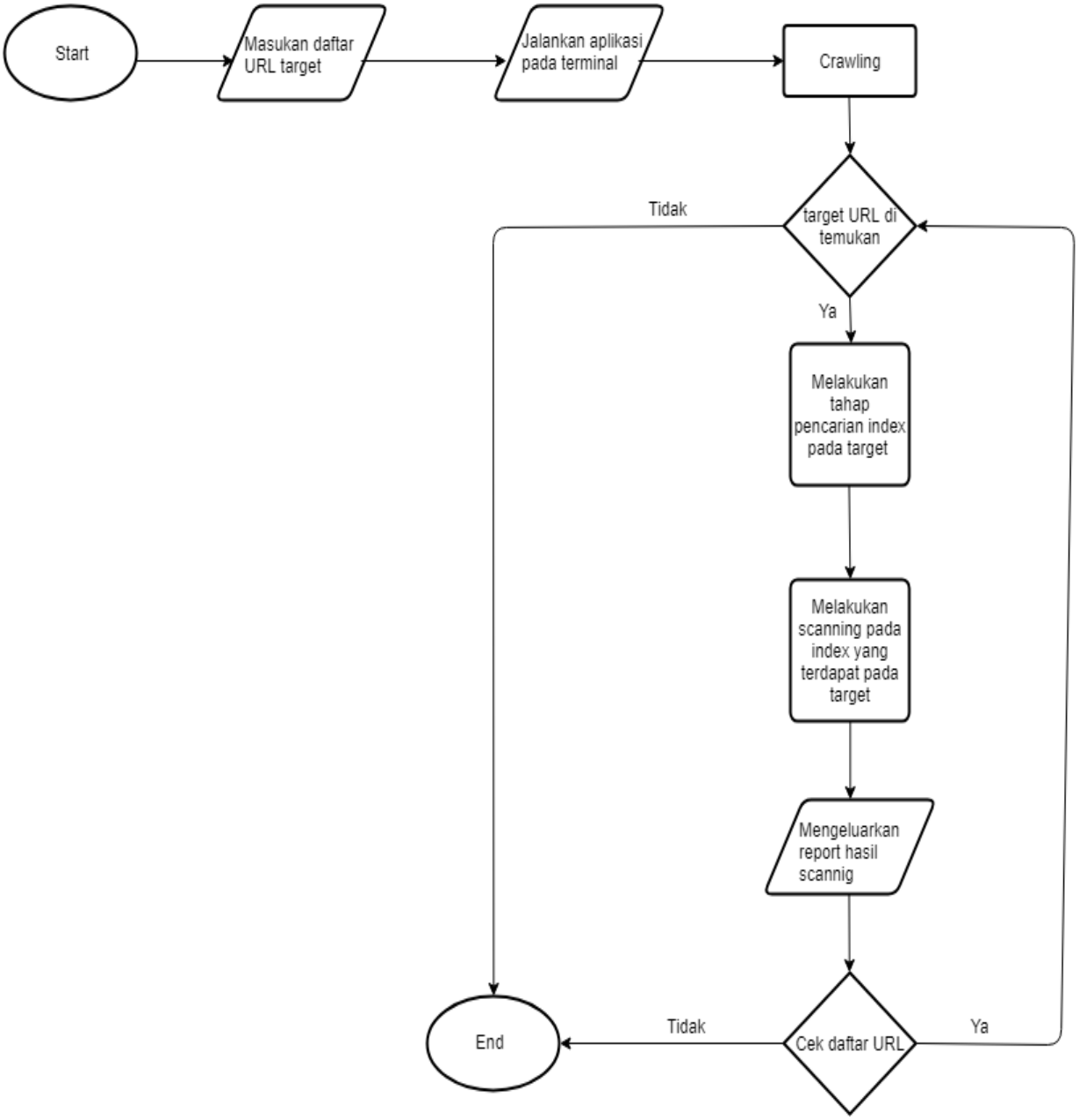
Setelah itu dari hasil pengujian akan didapatkan data dan *log* yang digunakan untuk analisis guna menemukan hasil akhir serta solusi yang tepat. Terakhir adalah pembuatan laporan akhir yang berisi semua tahapan-tahapan penelitian.

3.3 Kebutuhan Aplikasi

3.3.1 Otomatisasi OWASPZap

Aplikasi otomatisasi OWASPZap yang dikembangkan oleh penulis untuk membantu dalam proses *pentest* ini memiliki alur diagram (*flowchart*) seperti pada Gambar 3.2. Pada Gambar 3.2. hal pertama yang dilakukan adalah memasukan daftar nama-nama *web* yang akan dijadikan target kedalam halaman target.txt kemudian *user* menjalankan aplikasi pada terminal. Selanjutnya aplikasi akan melakukan proses *crawling* terhadap daftar target yang telah ditentukan sebelumnya yang dimasukan kedalam file target.txt setelah target ditemukan aplikasi akan melakukan proses pencarian terhadap semua *index* yang terdapat dalam *web* target.

Setelah semua *index* terdeteksi aplikasi akan melakukan *scanning* terhadap *index* target guna mencari celah keamanan setelah proses selesai aplikasi akan mengeluarkan *report* hasil *scanning* dan selanjutnya aplikasi akan melakukan pengecekan apakah masih ada daftar *URL* target dalam file target.txt jika semua daftar target sudah selesai dieksekusi dan sudah tidak terdapat daftar target lagi maka aplikasi akan berhenti namun jika masih ada target aplikasi akan mengulang proses seperti sebelumnya hingga semua daftar target dalam file target.txt selesai dieksekusi.



Gambar 3.2 Flowchart aplikasi Otomatisasi OWASPZap

3.3.2 Pseudocode

Pseudocode adalah algoritma yang sudah digabungkan dengan bahasa pemrograman yang digunakan (Pseudocode, 2017). *Pseudocode* pada umumnya digunakan karena dapat mempermudah perubahan notasi ke dalam bentuk bahasa pemrograman. *Library* dari *pseudocode* aplikasi otomatisasi OWASPZap dapat dilihat pada Tabel 3. 2 di bawah ini.

Tabel 3. 2 Library

N0	Nama *library*	Fungsi
1	import sys	Parameter yang berfungsi untuk menyediakan akses ke beberapa variable
2	import os	Modul yang berfungsi untuk berinteraksi dengan sistem operasi yang mendasari python
3	import subprocess	Modul yang bertujuan untuk mendefinisikan satu kelas dan beberapa fungsi yang menggunakan kelas yang sama agar dapat saling berkomunikasi
4	import time	Berisi fungsi dan class untuk operasi waktu
5	from pprint import pprint	Modul yang berfungsi untuk mengeluarkan output
6	From zapv2 import ZAPv2	Berfungsi untuk memanggil ZAPv2

Secara keseluruhan, algoritma aplikasi otomatisasi OWASPZap dapat dijelaskan dengan *pseudocode* yang terdapat pada Tabel 3. 3. Pada *pseudocode* tersebut terdapat beberapa kosakata yang digunakan antara lain Target, Jumlah Target, *Time*, ZAPv2. Variabel Target memiliki tipe data string dan digunakan untuk membaca data yang terdapat dalam file target.txt. Selanjutnya adalah variabel JumlahTarget yang bertipe data int berfungsi untuk mengindentifikasi jumlah target. Sedangkan *library* Time berfungsi untuk mengambil data waktu atau membuat variabel berdasarkan satuan waktu. selanjut ZAPv2 berfungsi untuk memanggil *library* Zap.

Tabel 3. 3 *Pseudocode* Aplikasi Otomatisasi OWASPZap

```
Aplikasi: Aplikasi Otomatisasi OWASPZap
Kamus:
Target : string
JumlahTarget :Int
Time : library
ZAPv2 : library
```

```
#Open Target File
    target = [line.rstrip('\n') for line in open('target.txt')]
    jumlahTarget = len(target)
    i = 0
    #targetScan = target
    while i<jumlahTarget:
  apikey = ''
     zap = ZAPv2(apikey=apikey)
  mainZap()
        zap.urlopen(target[i])
        # Give the sites tree a chance to get updated
        time.sleep(2)
        spiderScan(target[i])
        activeScan(target[i])
        showResults()
        i+=1
        time.sleep(5)
  # Shutting down ZaProxy daemon
  zap.core.shutdown()
```

Untuk deskripsi algoritma pada Tabel 3. 3 di atas pertama-tama pengguna diminta untuk memasukan alamat target ke dalam file target.txt. Selanjutnya ketika aplikasi dijalankan oleh pengguna aplikasi akan melakukan akses terhadap file target.txt kemudian akan dianalisa jumlah target yang ada dalam file target.txt.

Selanjutnya aplikasi akan melakukan pemanggilan *library* OWASPZap kemudian terdapat jeda 2 detik sebelum aplikasi akan melakukan proses *SpiderScan* terhadap target yang terdapat pada file target.txt proses *SpiderScan* bertujuan untuk mencari *direktory* yang terdapat dalam *web* target setelah proses ini selesai aplikasi akan melakukan *scanning* yang kedua yaitu *ActiveScan* untuk mencari kemungkinan celah keamanan yang terdapat dalam *web* target setelah proses *scanning* selesai aplikasi akan mencetak hasil dari proses *scanning* selanjutnya aplikasi akan melakukan perulangan jika masih terdapat target dalam file taget.txt jika sudah tidak ada maka aplikasi akan berhenti.

3.4 Analisis

Tahap ini bertujuan untuk melaporkan seluruh kegiatan dan hasil uji *penetrasi testing*. Lapora akan berupa laporan lisan dan laporan tertulis yang merinci seluruh kegiatan dan juga terdapat lampiran seluruh hasil uji termasuk didalamnya grafik, *tools* yang digunakan, celah keamanan yang ditemukan dan juga solusi untuk mengatasinya

3.5 Rekomendasi

Rekomendasi akan berbentuk tabel yang akan berisi jenis celah keamanan dan solusi untuk mengatasi celah keamanan tersebut sehingga nantinya bisa membatu admin dari *website* untuk melakukan tindakan pencegahan yang lebih dini terhadap celah-celah tersebut.

BAB IV
HASIL DAN PEMBAHASAN

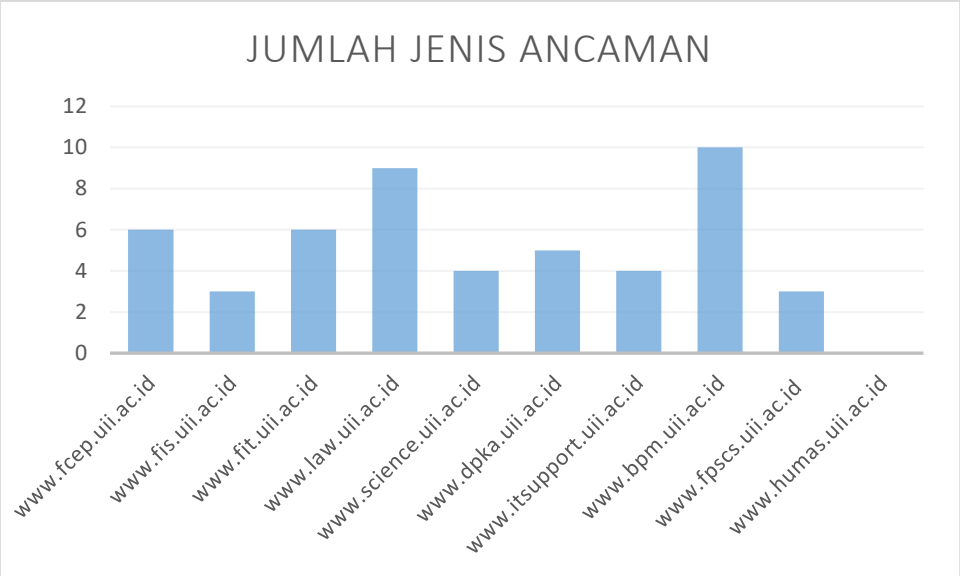
4.1 Hasil

Dari proses *scanning* yang telah dilakukan didapat hasil kemungkinan terdapat celah keamanan pada 10 *web* target yang berdomain uii.ac.id diantara seperti pada Gambar 4. 1

	fcep.uii.ac.id	fis.uii.ac.id	fit.uii.ac.id	fpscs.uii.ac.id	law.uii.ac.id	science.uii.ac.id	dpka.uii.ac.id	humas.uii.ac.id	itsupport.uii.ac.id	bpm.uii.ac.id
LOW	5	25	8	15	5	3	2	2	6	3
MEDIUM	3	7	6	5	3	3	3	2	4	3
HIGH	1	0	4	4	2	2	3	1	4	2

Gambar 4. 1 Celah keamanan pada domain uii.ac.id

Gambar 4.1 menunjukan grafik hasil *scanning* menggunakan aplikasi otomatisasi OWASPZap yang menujukan jumlah kemungkinan celah keamanan yang ada pada *web* target menurut level tingkat ancaman di sini terbagi menjadi 3 kategorikan berdasarkan efek yang ditimbulkan dari celah keamanan tersebut yaitu *High*, *Medium*, dan *Low*. Untuk detail ancaman yang terdapat pada tiap target dapat dilihat pada Tabel 4. 16. Selanjutnya hasil dari proses *scanning* menggunakan *tools* WPScan seperti yang ditunjukan pada Gambar 4. 2. Pada Gambar 4. 2 ini menjelaskan jumlah jenis kemungkinan celah keamanan yang terdapat dalam tiap *web*, pada grafik di bawah *web* www.humas.uii.ac.id tidak menunjukan hasil dikarena *web* bukan bertipe Wordpress seperti *web* lainya. Untuk melihat detail kemungkinan celah keamanan yang terdapat dalam *web* target dapat dilihat pada Tabel 4. 2 di bawah.



Gambar 4. 2 Jumlah jenis ancaman hasil scan dari WPScan

Hasil selanjutnya yang ditemukan dalam proses *scanning web* berdomain uii.ac.id ini juga ditemukan beberapa *user login* pada beberapa *web* target yang diduga merupakan *user login* dari target. *User login* yang ditemukan pada proses *scanning* diantaranya dapat dilihat pada Tabel 4. 3.

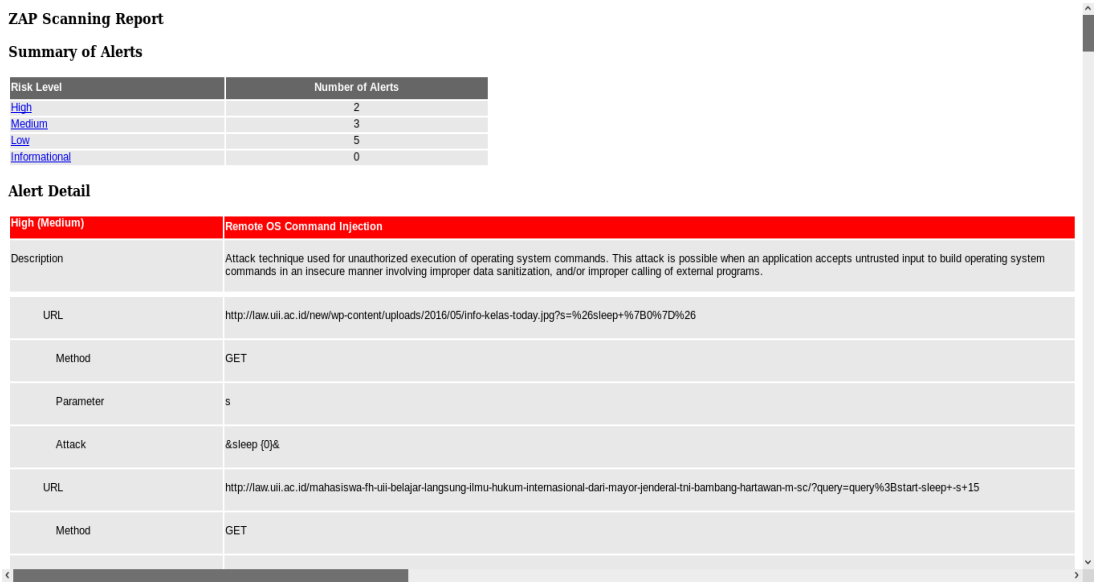
Tabel 4. 3 Hasil proses *scanning* menggunakan WPScan

URL	**User Login**
www.fis.uii.ac.id	*dm*n
	*arco*m
	ne*sw*iter
	a*mi*2
www.science.uii.ac.id	a*m*n
www.dpka.uii.ac.id	a*mi*
www.itsupport.uii.ac.id	i*5upp*rt
	*hep*x
	*nd*o
	rvi
	*li*ah
	*haf*ra
www.bpm.uii.ac.id	*pm*ii
www.fpscs.uii.ac.id	*psb*uii

URL	User Login
	*eb*aster

4.1.1 Aplikasi otomatisasi OWASP ZAP

Hasil *report* yang dikeluarkan aplikasi dalam format .html akan berupa tabel. Tabel paling atas berisikan risk level celah keamanan, jumlah celah yang dapat di deteksi dan tabel ke 2 berisikan level risk celah, kategori atau nama celah, lokasi celah berada, method, parameter dan juga yang terakhir solusi untuk menghadapi celah keamanan tersebut seperti yang ditunjukan pada Gambar 4. 3 dan Gambar 4. 4



ZAP Scanning Report

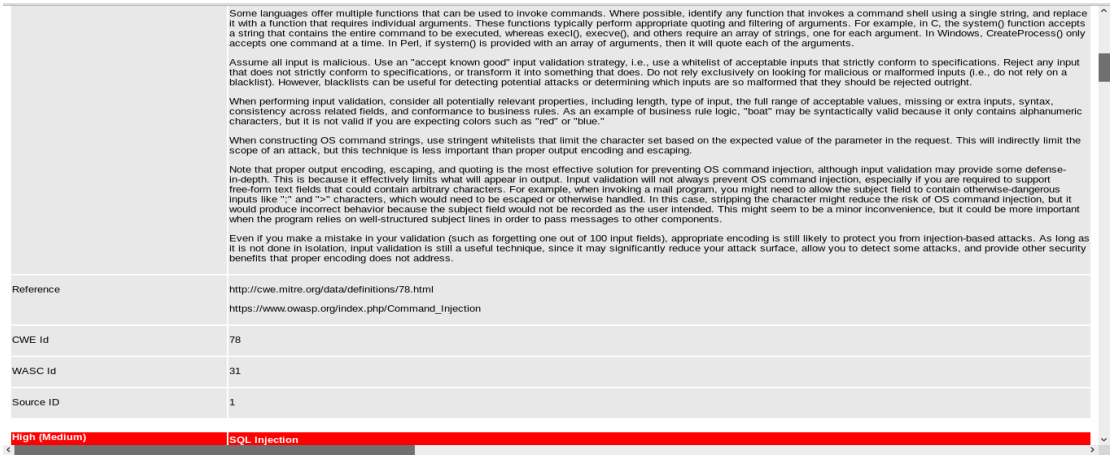
Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	3
Low	5
Informational	0

Alert Detail

High (Medium)	Remote OS Command Injection
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
URL	http://law.uii.ac.id/new/wp-content/uploads/2016/05/info-kelas-today.jpg?s=%26sleep+%7B0%7D%26
Method	GET
Parameter	s
Attack	&sleep {0}&
URL	http://law.uii.ac.id/mahasiswa-fh-uii-belajar-langsung-ilmu-hukum-internasional-dari-mayor-jenderal-tni-bambang-hartawan-m-sc/?query=query%3Bstart-sleep+-s+15
Method	GET

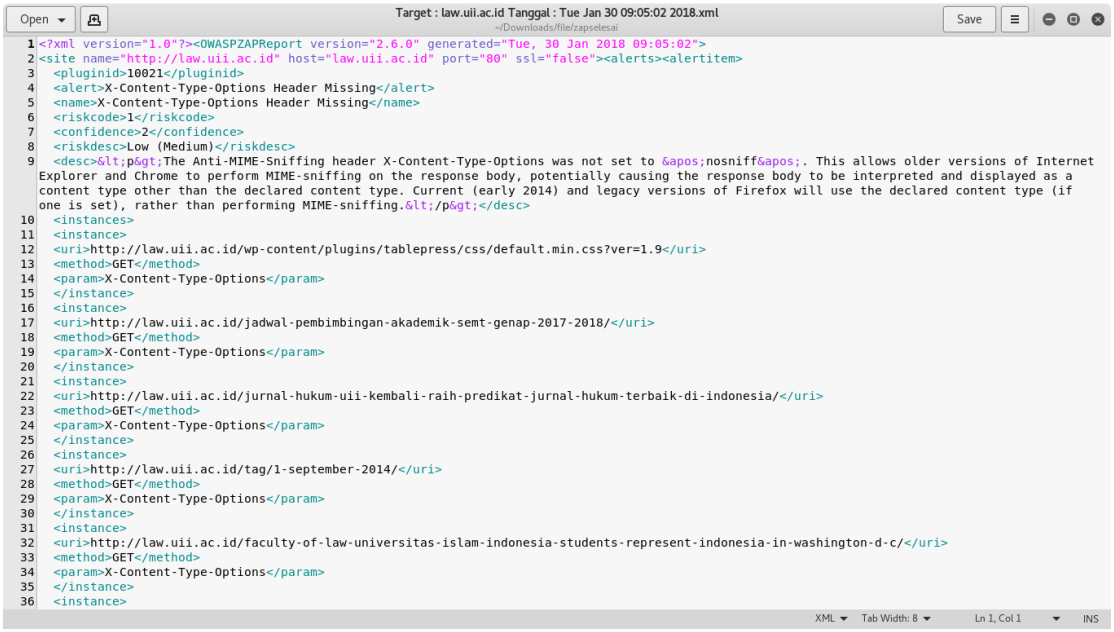
Gambar 4. 3 *Report* celah keamanan



	Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the system() function accepts a string that contains the entire command to be executed, whereas execl(), execve(), and others require an array of strings, one for each argument. In Windows, CreateProcess() only accepts one command at a time. In Perl, if system() is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." When constructing OS command strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://www.owasp.org/index.php/Command_Injection
CWE Id	78
WASC Id	31
Source ID	1
High (Medium)	SQL Injection

Gambar 4. 4 Solusi mengatasi celah keamanan

Sedangkan laporan dengan berformat xml berbeda tampilan dengan html tetapi memiliki isi yang sama seperti Gambar 4. 5 di bawah ini.




```
<?xml version="1.0"?><OWASPZAPReport version="2.6.0" generated="Tue, 30 Jan 2018 09:05:02">
<site name="http://law.uii.ac.id" host="law.uii.ac.id" port="80" ssl="false"><alerts><alertitem>
  <pluginid>10021</pluginid>
  <alert>X-Content-Type-Options Header Missing</alert>
  <name>X-Content-Type-Options Header Missing</name>
  <riskcode>1</riskcode>
  <confidence>2</confidence>
  <riskdesc>Low (Medium)</riskdesc>
  <desc>&lt;p&gt;The Anti-MIME-Sniffing header X-Content-Type-Options was not set to &apos;nosniff&apos;. This allows older versions of Internet
Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a
content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if
one is set), rather than performing MIME-sniffing.&lt;/p&gt;</desc>
  <instances>
  <instance>
  <uri>http://law.uii.ac.id/wp-content/plugins/tablepress/css/default.min.css?ver=1.9</uri>
  <method>GET</method>
  <param>X-Content-Type-Options</param>
  </instance>
  <instance>
  <uri>http://law.uii.ac.id/jadwal-pembimbingan-akademik-semt-genap-2017-2018/</uri>
  <method>GET</method>
  <param>X-Content-Type-Options</param>
  </instance>
  <instance>
  <uri>http://law.uii.ac.id/jurnal-hukum-uii-kembali-raih-predikat-jurnal-hukum-terbaik-di-indonesia/</uri>
  <method>GET</method>
  <param>X-Content-Type-Options</param>
  </instance>
  <instance>
  <uri>http://law.uii.ac.id/tag/1-september-2014/</uri>
  <method>GET</method>
  <param>X-Content-Type-Options</param>
  </instance>
  <instance>
  <uri>http://law.uii.ac.id/faculty-of-law-universitas-islam-indonesia-students-represent-indonesia-in-washington-d-c/</uri>
  <method>GET</method>
  <param>X-Content-Type-Options</param>
  </instance>
  <instance>
```

Gambar 4. 5 *Report* celah keamanan format xml

4.2 Pembahasan

4.2.1 Aplikasi otomatisasi OWASP ZAP

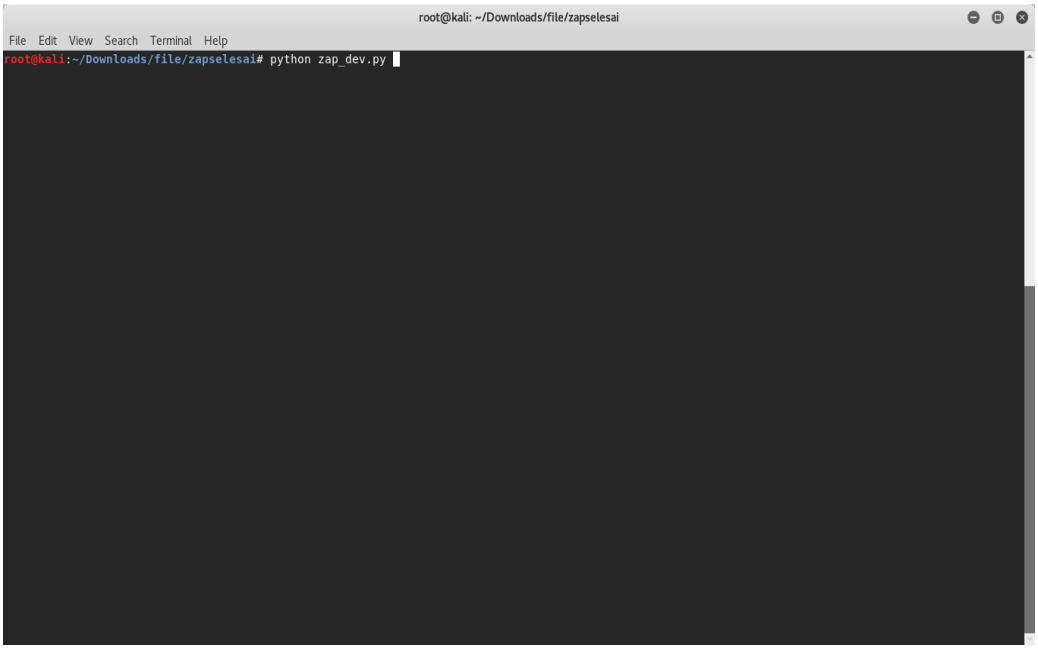
Pada tahap ini akan dijelaskan penggunaan aplikasi otomatisasi OWASPZap. Tampilan aplikasi seperti Gambar 4. 6 di bawah ini yang berisikan 2 file yaitu target.txt dan zap_dev.py.

Gambar 4. 6 File aplikasi otomatisasi OWASPZap

Pertama user membuka file target.txt dan memasukan daftar *URL* target yang akan dilakukan *scanning* seperti Gambar 4. 7. Di sini penulis mencontohkan menggunaka 10 *URL web* untuk dilakukan proses *scanning*

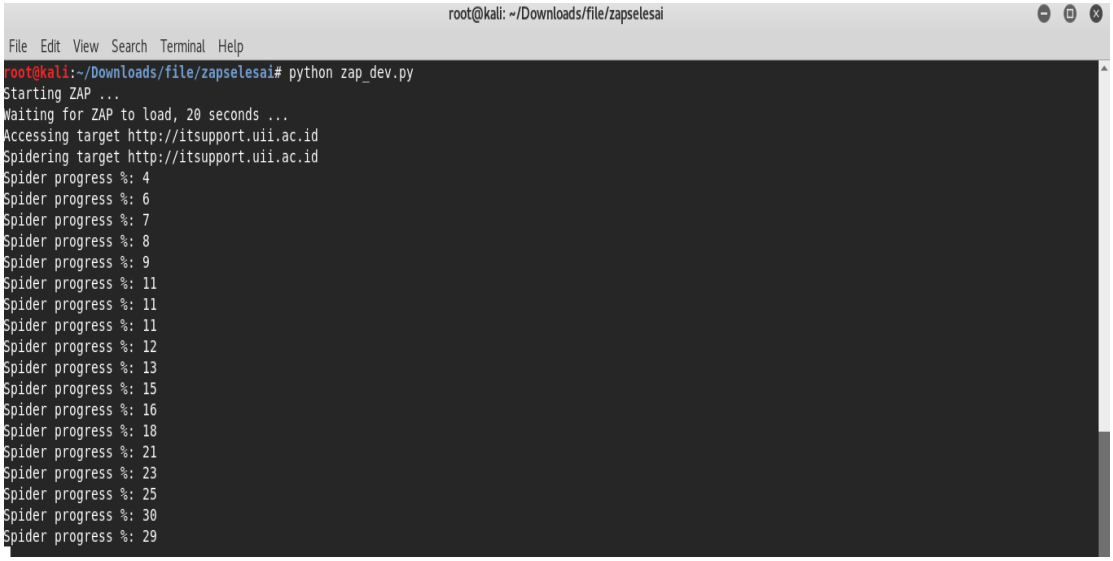
Gambar 4. 7 URL Target

Setelah user memasukan *URL* target seperti Gambar 4. 8 langkah selanjutya adalah membuka terminal dan menjalankan aplikasi pada terminal seperti Gambar 4. 9 di bawah ini

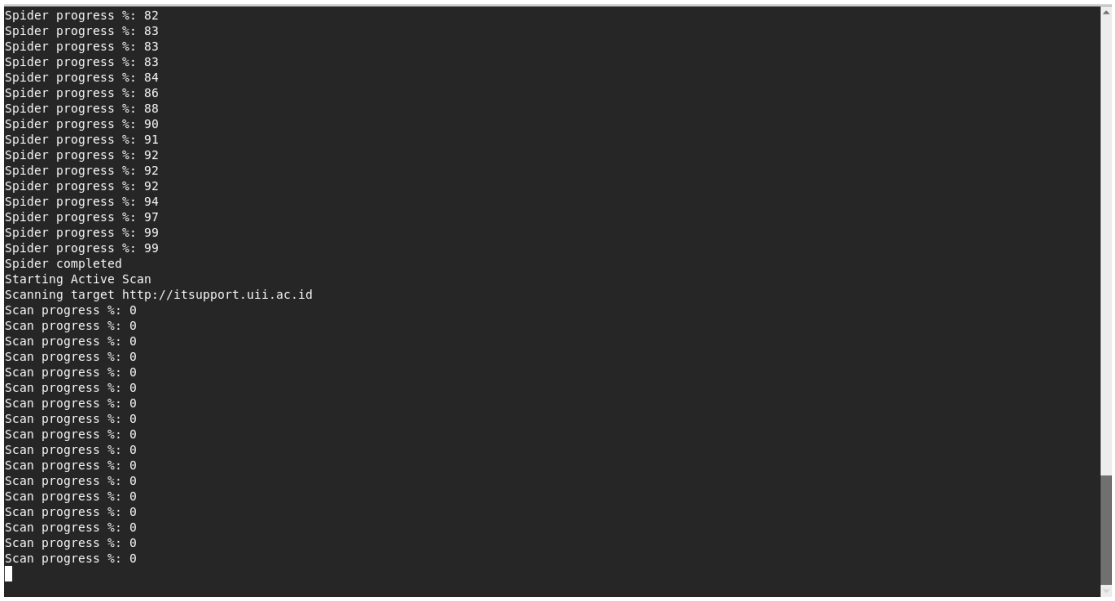


Gambar 4. 8 Proses memasukkan URL target

Setelah dijalankan aplikasi akan melakukan pencarian *web* target (*crawling*) dan melakukan proses *scanning* awal untuk mengidentifikasi semua *index* yang terdapat dalam *web* target yang ditunjukan seperti Gambar 4. 9 pada proses *SpiderScan*.

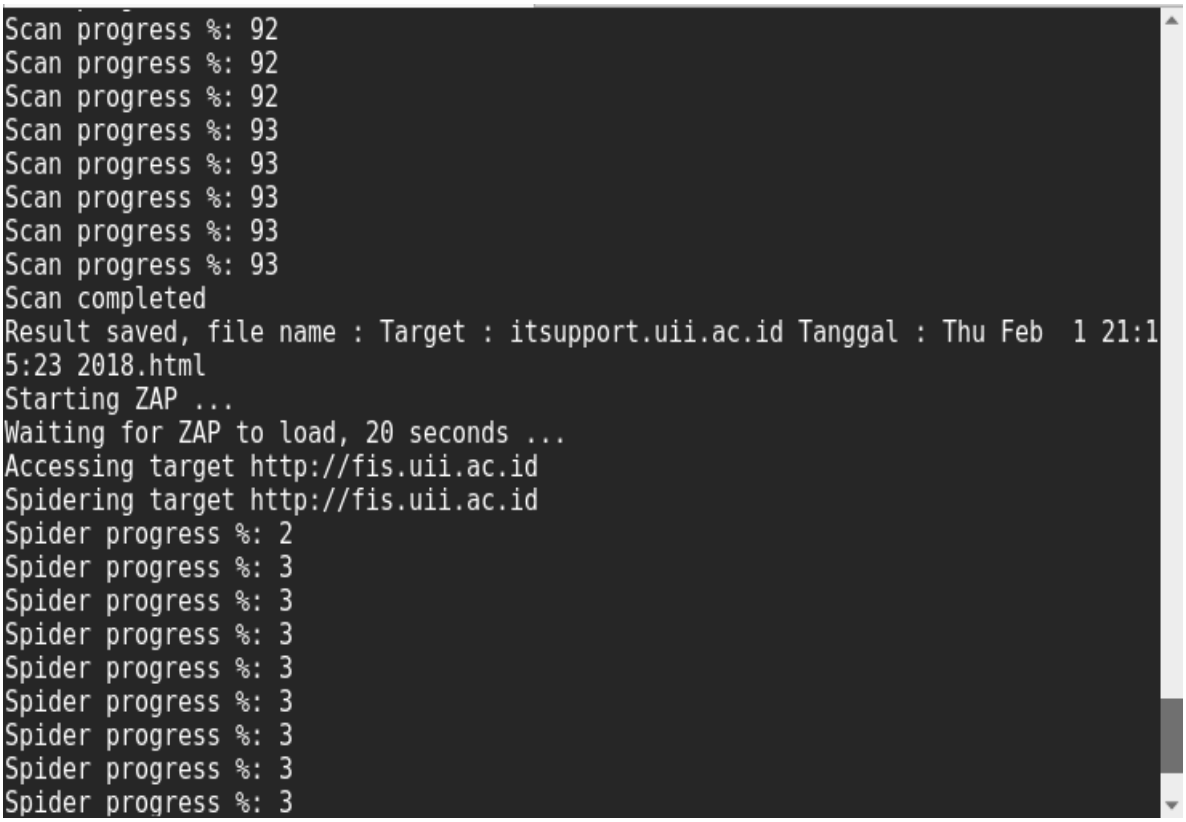


Gambar 4. 9 Proses *SpiderScan* aplikasi otomatisasi OWASPZap



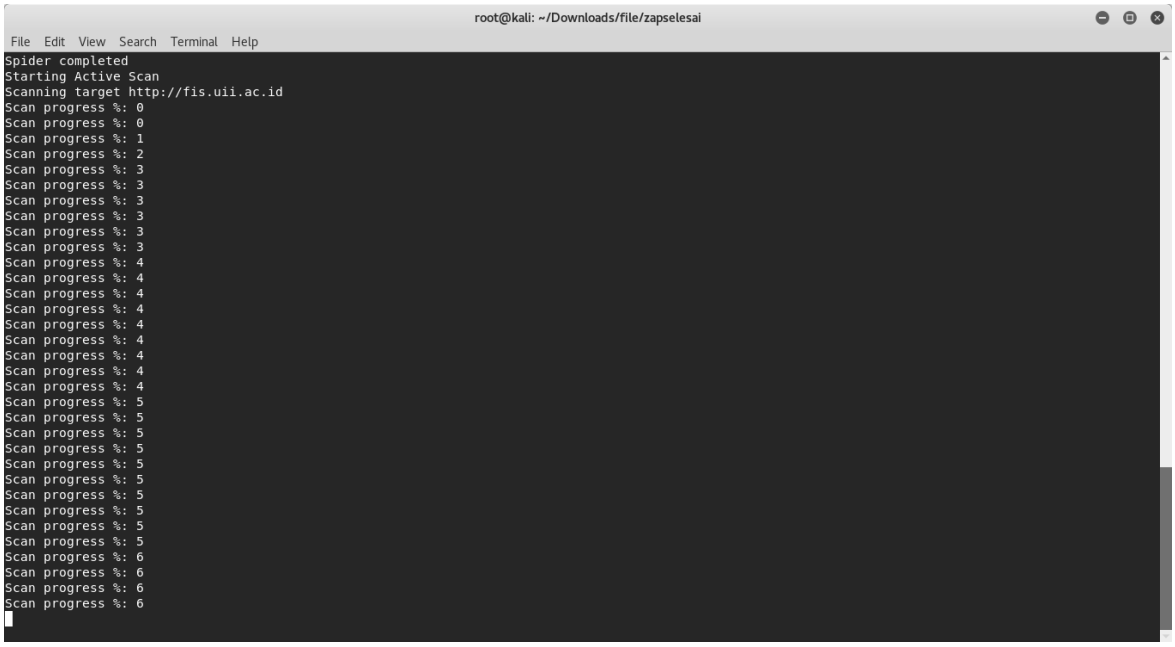
Gambar 4. 10 Proses *scan* otomatisasi OWASPZap.

Tahap selanjutnya setelah proses *spider progress* atau pengindentifikasian semua *index* selesai dan mendapatkan *index* yang terdapat dalam *web* target secara otomatis akan ke tahap selanjutya adalah *scan progress* yang ditunjukan pada Gambar 4. 11 tahap ini bertujuan untuk pencarian celah keamanan pada *web* target.



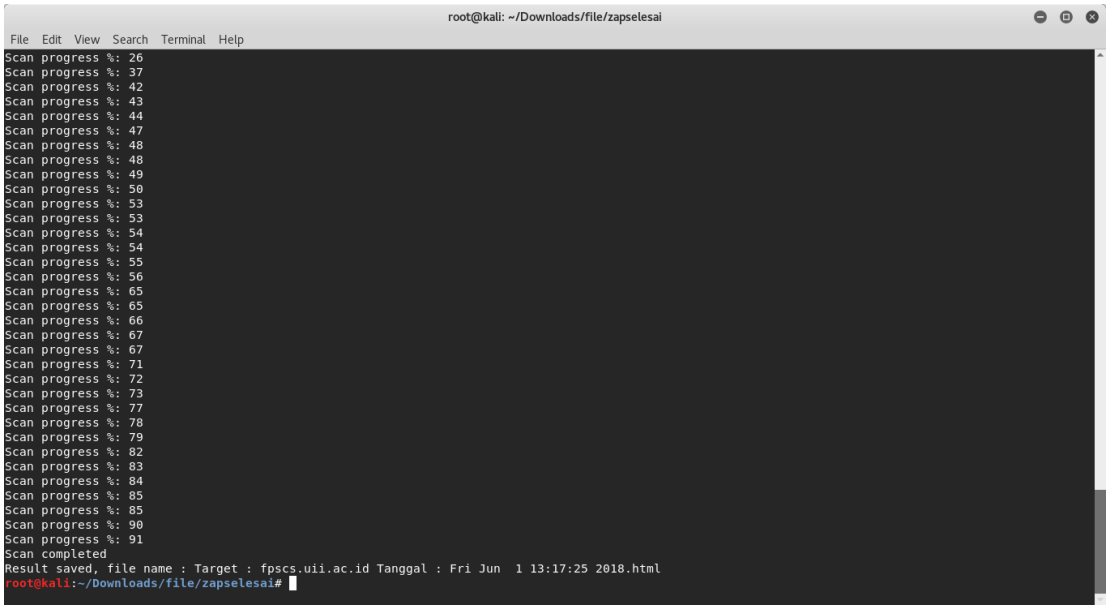
Gambar 4. 11 Proses *spiderScan* dari aplikasi otomatisasi OWASPZap

Setelah tahap *scan progress* selesai aplikasi akan mengeluarkan *result* atau hasil *scanning* dari *web* target. File yang dikeluarkan akan disimpan dengan format nama target serta tanggal dan jam proses *scanning* selesai dilakukan seperti Gambar 4. 11 proses selanjutnya aplikasi akan melakukan otomatisasi *scanning* pada target selanjutnya seperti yang ditunjukan pada Gambar 4. 7 di sini penulis menggunakan 10 contoh *web* target untuk dilakukan proses *scanning.* Di sini aplikasi akan melakukan proses *crawling* terlebih dahulu seperti proses sebelumnya selanjutnya akan dilakukan pencarian *index* pada *web* target atau yang disebut *spider progresss* seperti yang ditunjukan Gambar 4. 11 di atas setelah prosess pencarian *index* atau *spider progress* selesai akan dilakukan proses *scanning* berikutnya pada *web* target untuk menemukan celah keamanan pada *index* yang terdapat pada *web* target yang ditunjukan Gambar 4. 12 di bawah.



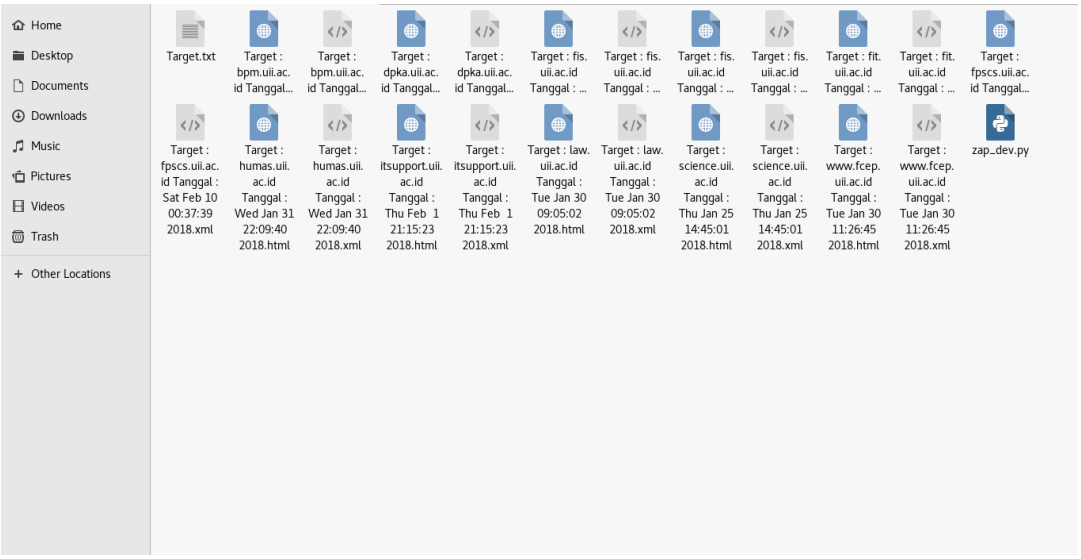
Gambar 4. 12 Proses *ActiveScan* dari aplikasi otomatisasi OWASPZap

Tahap selanjutnya setelah aplikasi selesai melakukan *scanning* akan mengeluarkan laporan. Kemudian aplikasi akan kembali mengulang semua proses sebelumnya seperti pada Gambar 4. 12 dan aplikasi akan mengulang proses tersebut hingga semua daftar target dalam file Target.txt telah dieksekusi.



Gambar 4. 13 Proses *scan* menggunakan aplikasi otomatisasi OWASPZap

Kemudian jika semua *web* target yang dimasukan dalam daftar sudah tidak ada maka aplikasi akan secara otomatis berhenti seperti Gambar 4. 13. Hasil dari proses *scanning* ini terdapat 2 file yaitu file dengan format html dan xml dengan isi yang sama pada kedua format seperti dapat dilihat di Gambar 4. 14 di bawah ini.



Gambar 4. 14 Hasil keluaran aplikasi otomatisasi OWASPZap

4.2.2 Implementasi Otomatisasi OWASP ZAP

Hasil code program dari aplikasi otomatisasi OWASPZap ini dapat dilihat pada Tabel 4. 3 . Kode pada baris 1 hingga 26 digunakan untuk menampilkan proses berjalanya program pada terminal hal-hal yang ditampilkan berupa setatus proses *scanning* yang sedang berjalan berupa persen dan pesan *scanning* telah selesai. Selanjutnya kode baris 30 sampe dengan 46 berisikan kode program yang berfungsi mengeluarkan laporan hasil *scanning* yang akan dikeluarkan dalam 2 bentuk file bertipe .html dan .xml yang akan disimpan dengan format nama berbentuk nama target yang diuji dan tanggal selesai proses scan.

Tabel 4. 4 Source code program

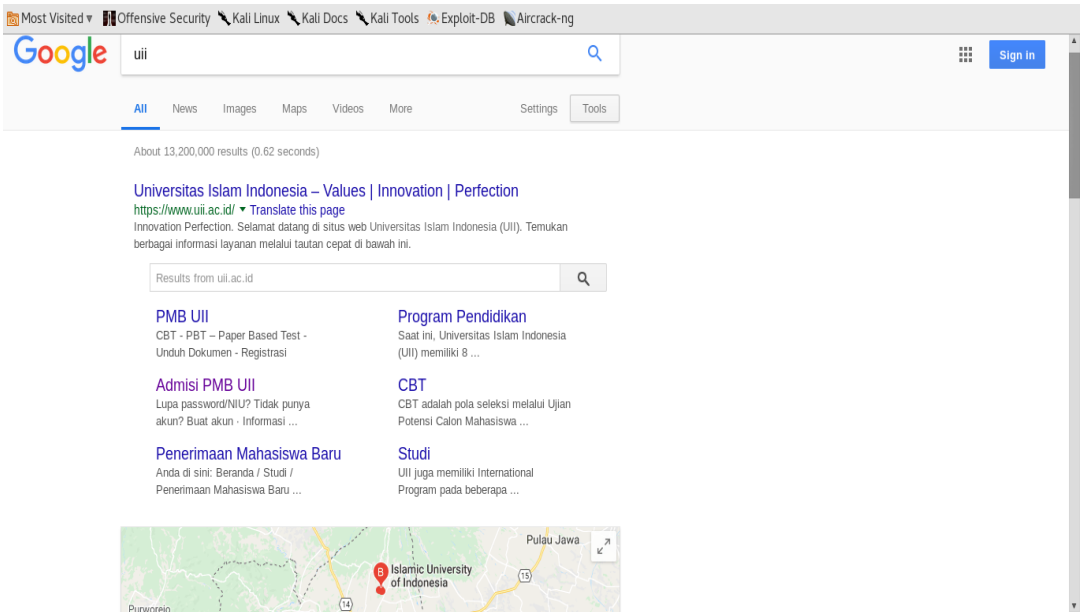
```
1  # Active Scan Module
2  def activeScan(targetScan):
3      # do stuff
4      print 'Starting Active Scan'
5      print 'Scanning target %s' % target[i]
6      scanid = zap.ascan.scan(target[i])
```

```
7       #Show Active Scan Progress
8       while (int(zap.ascan.status(scanid)) < 100):
9           print 'Scan progress %: ' + zap.ascan.status(scanid)
10          # Give enough time for Active Scan to finish
11          time.sleep(5)
12      print 'Scan completed'
13      return
14  # Spider Scan module
15  def spiderScan(targetScan):
16      # do stuff
17      print 'Accessing target %s' % target[i]
18      # try have a unique enough session...
19      print 'Spidering target %s' % target[i]
20      scanid = zap.spider.scan(target[i])
21      # Give the Spider a chance to start
22      time.sleep(2)
23      while (int(zap.spider.status(scanid)) < 100):
24          print 'Spider progress %: ' +
25  zap.spider.status(scanid)
26          time.sleep(2)
27      print 'Spider completed'
28      # Give the passive scanner a chance to finish
29      time.sleep(5)
30      return
31  def showResults():
32      #print ('Hosts: ' + ', '.join(zap.core.hosts))
32      #print ('Sites: ' + ', '.join(zap.core.sites))
34      #print ('Urls: ' + ', '.join(zap.core.urls))
35      #print ('Alerts: ')
36      #pprint (zap.core.alerts())
37      # Writes the XML and HTML reports that will be exported to
38  the workspace.
39      fileName1 = time.strftime("%c")
40      fileName2 =
41  target[i].replace("http://","").replace("/",("-"))
42
```

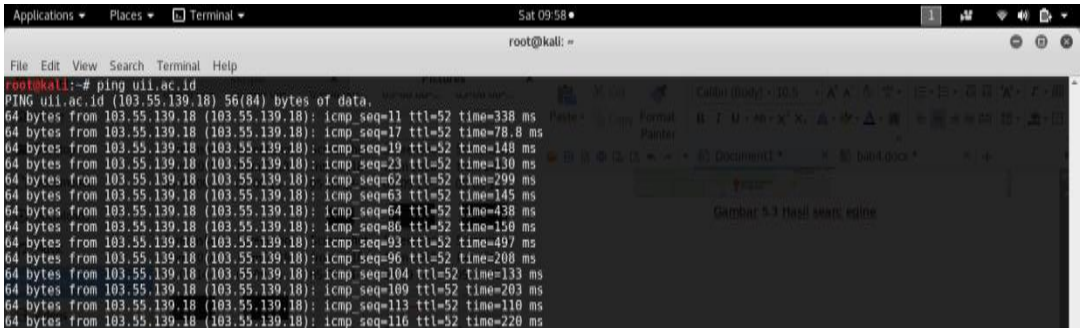
```
43      f = open('Target : '+fileName2+' Tanggal :
44  '+fileName1+'.xml','w')
45      f2 = open('Target : '+fileName2+' Tanggal :
46  '+fileName1+'.html','w')
        f.write(zap.core.xmlreport(zap))
        f2.write(zap.core.htmlreport(zap))
        f.close()
        f2.close()
        print 'Result saved, file name : '+'Target : '+fileName2+'
    Tanggal : '+fileName1+'.html'
```

4.3 Analisis

Pada tahap awal ini penulis menggunakan beberapa *tools* untuk mencari informasi tentang *web* target yang akan dilakukan uji *pentest*. Dengan menggunakan *search engine* yaitu Google seperti terlihat pada Gambar 4. 15. Pada Gambar 4. 15 didapatkan bahwa UII memiliki situs utama yaitu https://www.uii.ac.id/. Dengan menggunakan perintah ping seperti Gambar 4. 16 didapatkan bahwa uii.ac.id memiliki *IP* address 103.55.139.18.



Gambar 4. 15 Hasil pencarian informasi menggunakan Google.com

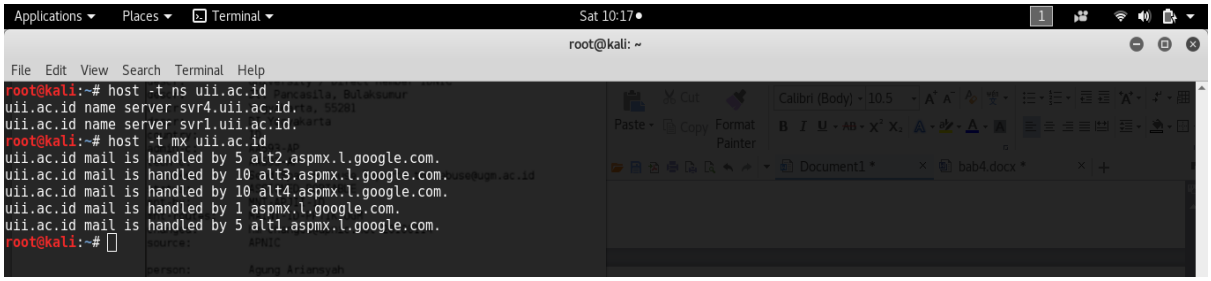


Gambar 4. 16 Hasil perintah ping

Selanjutnya menggunakan *tools* whois didapatkan hasil seperti Gambar 4. 17 .Dari Gambar terlihat bahwa uii.ac.id memiliki *block IP adders* dari 103.55.139.0 sampai dengan 103.55.139.255. Selain block alamat *IP* juga didapatkan nama, *email* dan kontak pengelola *server*.

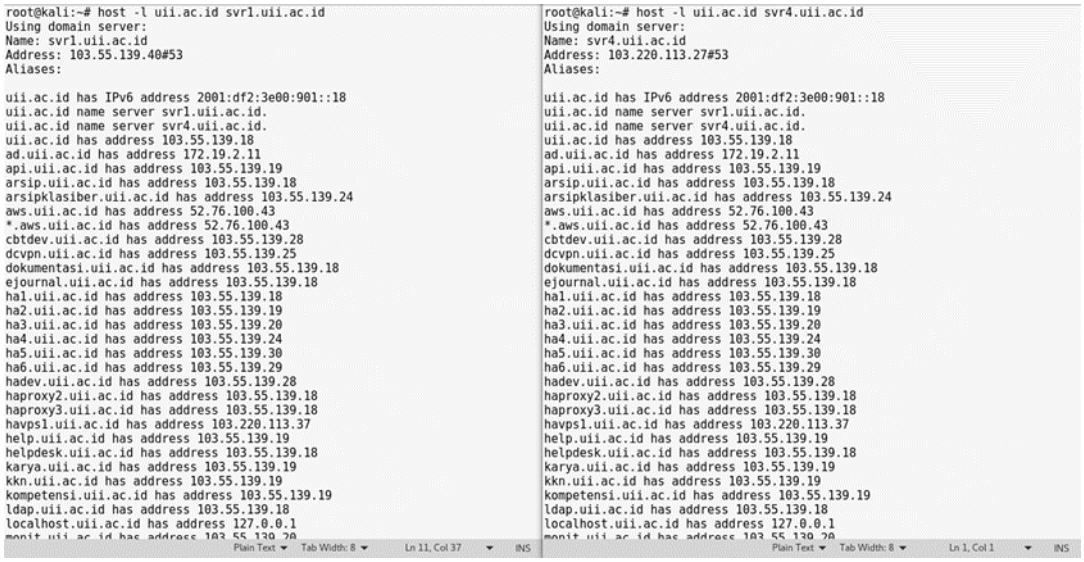
Gambar 4. 17 Hasil WhoIs

Dengan menggunakan perintah host didapatkan nama *server* dari UII yaitu svr4.uii.ac.id, svr1.uii.ac.id dan juga didapatkan *mail server* yang bertanggung jawab untuk domain uii.ac.id yaitu seperti Gambar 4. 18



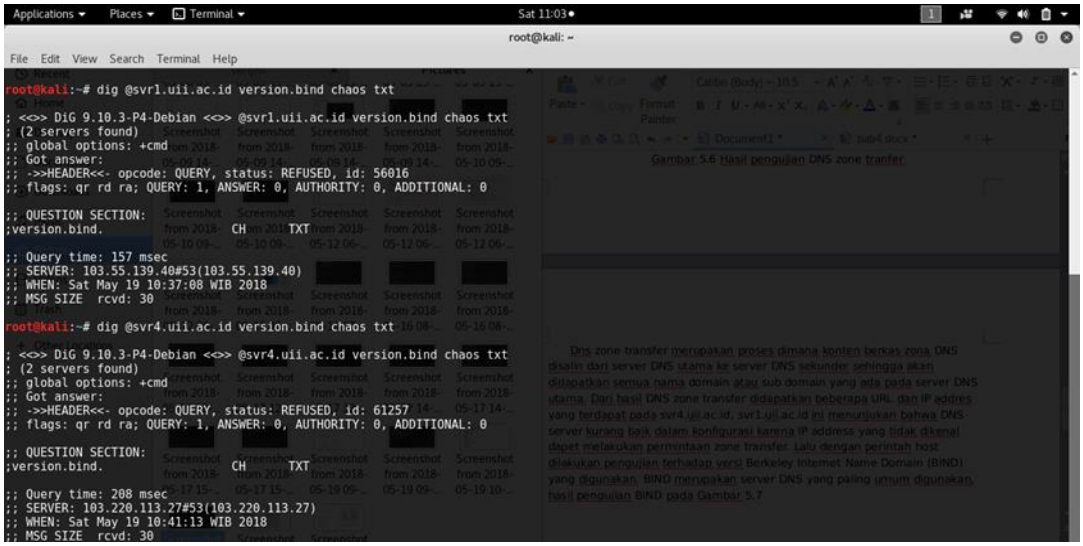
Gambar 4. 18 Hasil host

Dari informasi yang didapatkan tersebut dilanjutkan dengan mencoba melakukan pengujian *Domain Name Server (DNS) zone transfer* untuk seluruh informasi dari uii.ac.id seperti Gambar 4. 19 di bawah ini.



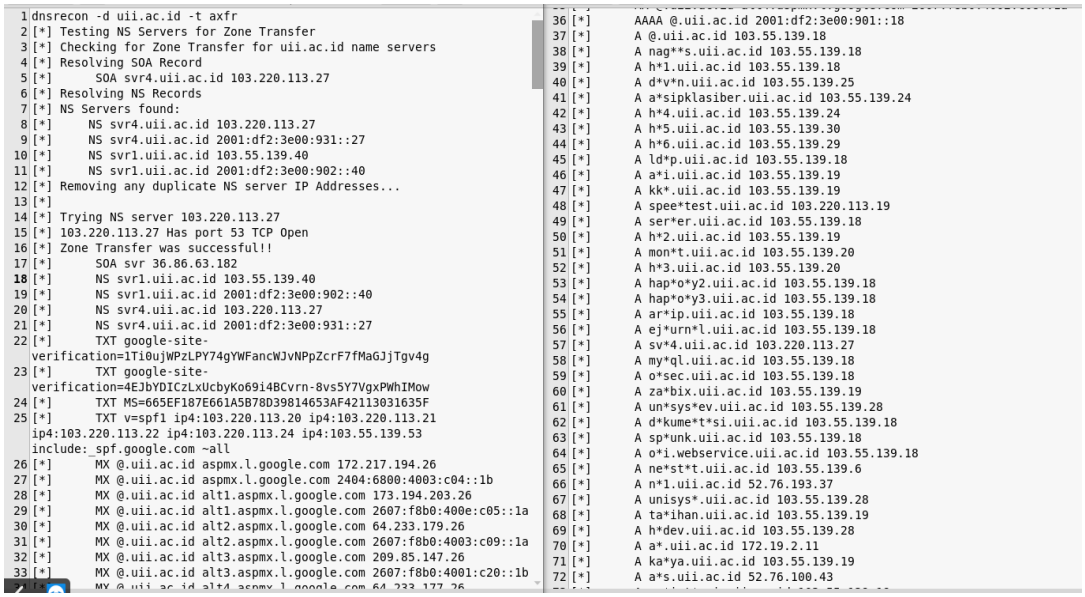
Gambar 4. 19 Hasil *DNS Zone Transfer*

DNS zone transfer merupakan proses dimana konten berkas *zona DNS* disalin dari *server DNS* utama ke *server DNS* sekunder sehingga akan didapatkan semua nama domain atau sub domain yang ada pada *server DNS* utama. Dari hasil *DNS zone transfer* didapatkan beberapa *URL* dan *IP addres* yang terdapat pada svr4.uii.ac.id, svr1.uii.ac.id hasil ini menunjukan bahwa *DNS server* belum dikonfigurasi dengan baik karena masih mengijinkan sembarang *IP address* melakukan permintaan *zone transfer*. Lalu dengan perintah host dilakukan pengujian terhadap versi *Berkeley Internet Name Domain (BIND)* yang digunakan. *BIND* merupakan *server DNS* yang paling umum digunakan, hasil pengujian *BIND* pada Gambar 4.20



Gambar 4. 20 Hasil uji menggunakan BIND

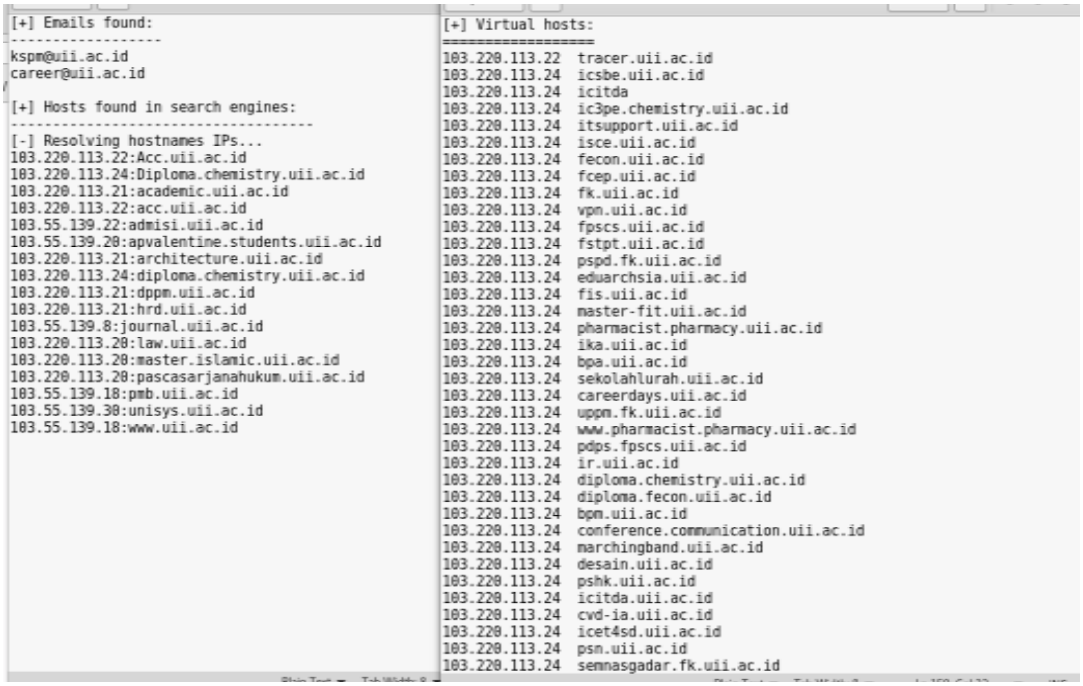
Dari hasil pengujian BIND *server* tidak menjawab permintaan untuk versi BIND yang digunakan. Pengujian selanjutnya menggunakan *tools dnsrecon* menunjukkan hasil seperti pada Gambar 4. 21



Gambar 4. 21 Hasil pengujian dengan *dnsrecon*

Dengan menggunakan *dnsrecon*, didapatkan informasi dari *DNS server* akan tetapi *web* target yang dicari penulis tidak didapatkan. Langkah berikutnya dengan cara mendapatkan informasi dengan cara *crawling* di internet. Terdapat beberapa *tools* yang memiliki kemampuan untuk mengumpulkan informasi secara otomatis dari internet melalui *search engine* dengan memasukkan *syntax* yang diinginkan. Gambar 4. 22 menunjukkan hasil

crawling menggunakan *tools* Theharvester dimana mendapatkan *email address, subdomain,* dan juga *virtual host* dari sistem dan jaringan UII.



Gambar 4. 22 Hasil *crawling*

Penulis berhasil menemukan *website* yang akan menjadi target *penetration testing*, dengan memilih acak 6 *website* fakultas, 2 *website* direktorat dan 2 *website* badan yang terdapat di UII seperti Tabel 4. 5

Tabel 4. 5 Daftar target

NO	FAKULTAS	Direktorat	Badan
1	www.fcep.uii.ac.id	www.dpka.uii.ac.id	www.itsupport.uii.ac.id
2	www.fis.uii.ac.id	www.humas.uii.ac.id	www.bpm.uii.ac.id
3	www.fit.uii.ac.id		
4	www.fpscs.uii.ac.id		
5	www.law.uii.ac.id		
6	www.science.uii.ac.id		

4.3.1 *Network Mapping*

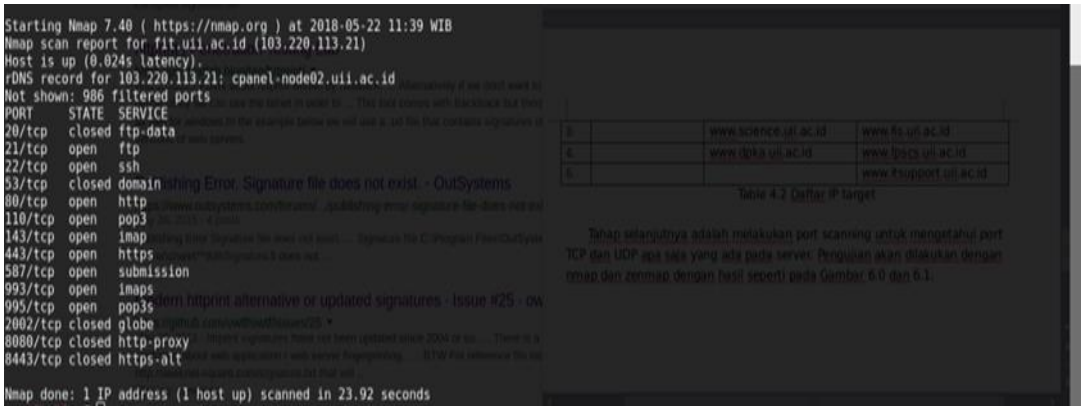
Pada tahap *network mapping* ini akan lebih memfokuskan interaksi langsung dengan perangkat atau sistem jaringan dari target yang akan dilakukan *pentest*. Pertama karena target

memiliki *IP* yang berupa *Virtual Host* maka target dikelompokan menjadi satu sesuai *IP* yang dimiliki seperti Tabel 4. 6

Tabel 4. 6 Daftar *IP* Target

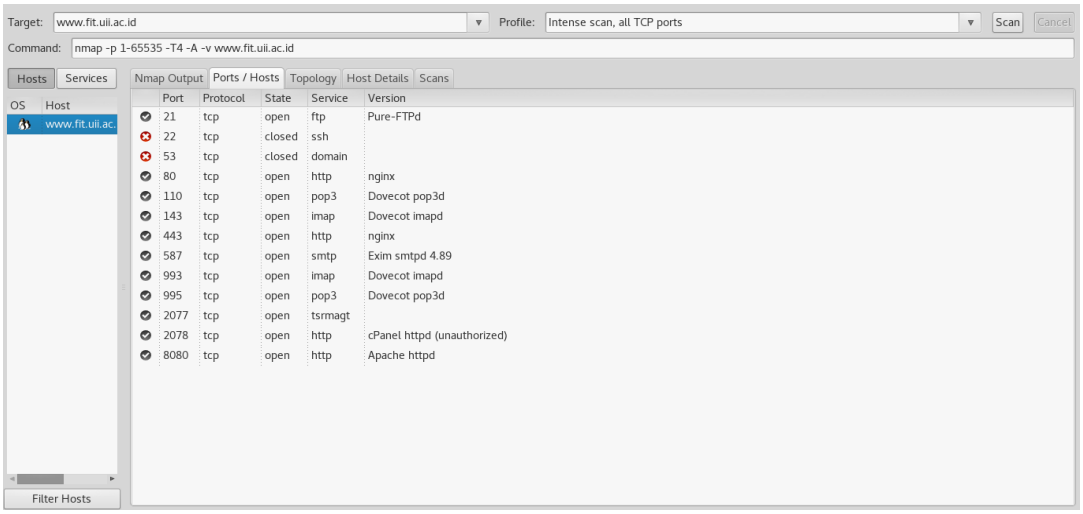
	IP		
No	103.220.113.20	103.220.113.21	103.220.113.24
1.	www.law.uii.ac.id	www.fit.uii.ac.id	www.bpm.uii.ac.id
2.		www.humas.uii.ac.id	www.fcep.uii.ac.id
3.		www.science.uii.ac.id	www.fis.uii.ac.id
4.		www.dpka.uii.ac.id	www.fpscs.uii.ac.id
5.			www.itsupport.uii.ac.id

Tahap selanjutnya adalah melakukan *port scanning* untuk mengetahui *port* TCP dan UDP apa saja yang ada pada *server*. Pengujian akan dilakukan dengan *tools* nmap dan zenmap dengan hasil seperti pada Gambar 4. 23 dan Gambar 4. 24.



Gambar 4. 23 Hasil *port scanning* dengan nmap

Hasil nmap dengan mode -sT atau TCP connect scan menunjukan daftar *port* TCP yang terbuka antara lain *port* 21 untuk layanan FTP, 22 untuk layanan SSH, *port* 80 untuk layanan HTTP, *port* 110 untuk POP3, *port* 143 IMAP, *port* 443 HTTPS, *port* 587 untuk SUBMISSION, *port* 993 untuk IMAPS dan 995 untuk POP3.



Gambar 4. 24 Hasil *port scanning* dengan zenmap

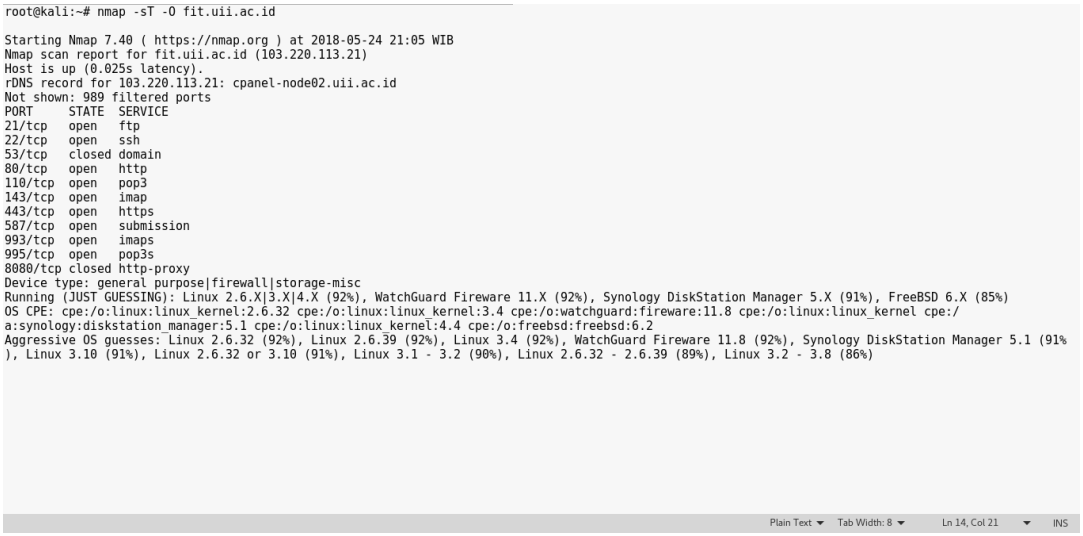
Pada hasil *scanning* menggunakan zenmap dengan profile Intense scan, all TCP *ports* menunjukan hasil yang sedikit berbeda dan jumlah *port* yang terdeteksi lebih banyak dibanding menggunakan nmap. Melihat hasil *scanning* dari nmap dan zenmap terdapat beberapa kesamaan *port* dengan default *port* pada pengaturan CPanel dan besar kemungkinan dalam *web* target terdapat CPanel. Selanjutnya akan dilakukan *scanning* pada *port* UDP dengan menggunakan netcut dan nmap yang mana tidak ditemukan hasil *port* UDP yang terbuka ada kemungkinan paket UDP terhalangi oleh firewall yang terdapat dalam jaringan.

Karena dicurigai terdapat *firewall* maka akan dilakukan pengujian untuk memastikan ada atau tidaknya keberadaan *firewall* dengan menggunakan *tools* nmap. Tipe *scanning* yang akan dilakukan dengan FIN/ACK scan atau *maimon scan* yang mana menunjukan tahap akhir pada three-way handshake. Hasil *scanning* pada Gambar 4. 25 menunjukan bawah *server* fit.uii.ac.id memiliki *port* 22 terbuka yang hasil *scanning* sebelumnya memiliki perbedaan dan melakukan pengujian terhadap *port* 80 hasil dari 2 pengujian tersebut memverifikasi keberadaan *firewall* dengan menunjukan statet open|filtered pada *port* 22 dan 80.

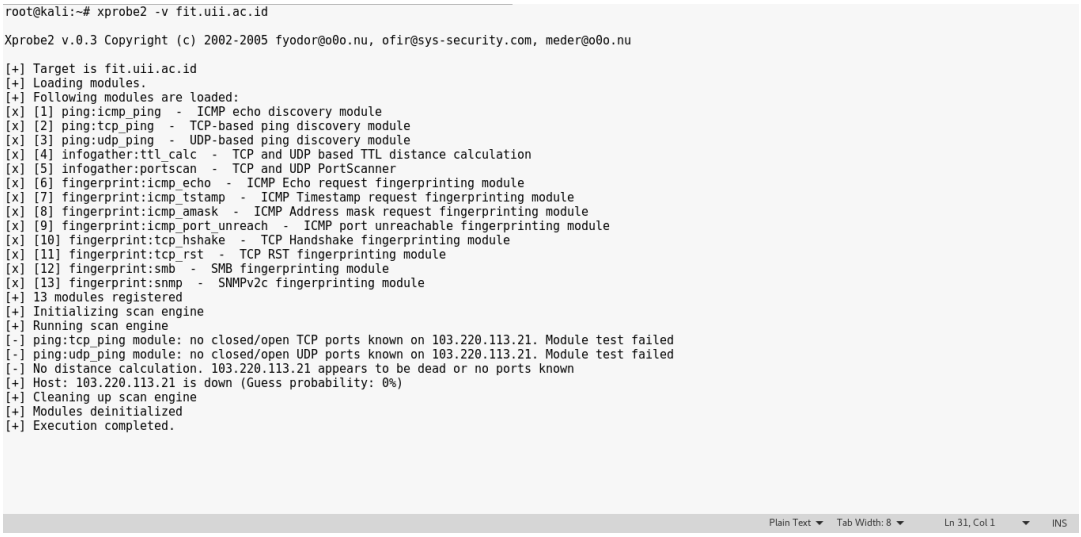
```
root@kali:~# nmap -sM -p22,80 103.220.113.21

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-22 13:09 WIB
Nmap scan report for cpanel-node02.uii.ac.id (103.220.113.21)
Host is up (0.0042s latency).
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
```

Gambar 4. 25 Hasil maimon scan

Tahap selanjutnya akan dilakukan OS fingerprinting untuk mengetahui jenis sistem operasi yang digunakan pada *server* fit.uii.ac.id. Pengujian OS fingerprinting akan digunakan *tools* nmap, xprobe2 dan zenmap. Hasil nmap pada Gambar 4. 26 menunjukan bahwa sistem operasi yang digunakan adalah Linux 2.6.32 dengan tingkat akurasi sebesar 92% dan menggunakan *tools* xprobe2 tidak didapatkan informasi mengenai versis os target seperti ditunjukan Gambar 4. 27 di bawah ini.

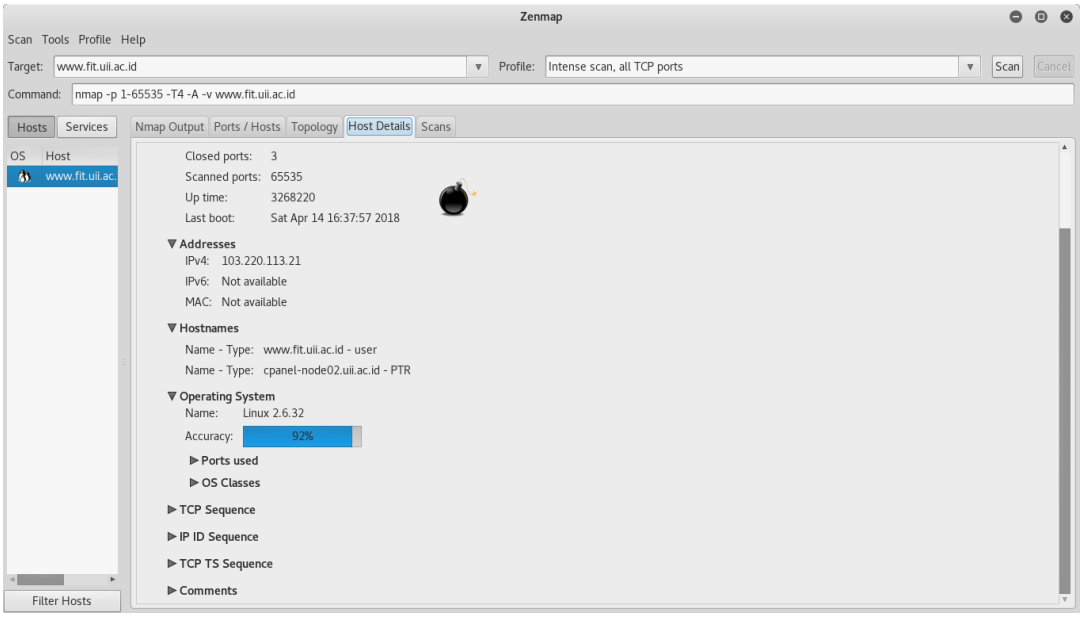


Gambar 4. 26 Fingerprinting dengan nmap



Gambar 4. 27 OS fingerprinting dengan xpobe2

Selanjutnya menggunakan *tools* zenmap didapatkan hasil Linux 2.6.32 dengan tingkat akurasi sebesar 92% pada Gambar 4. 28.



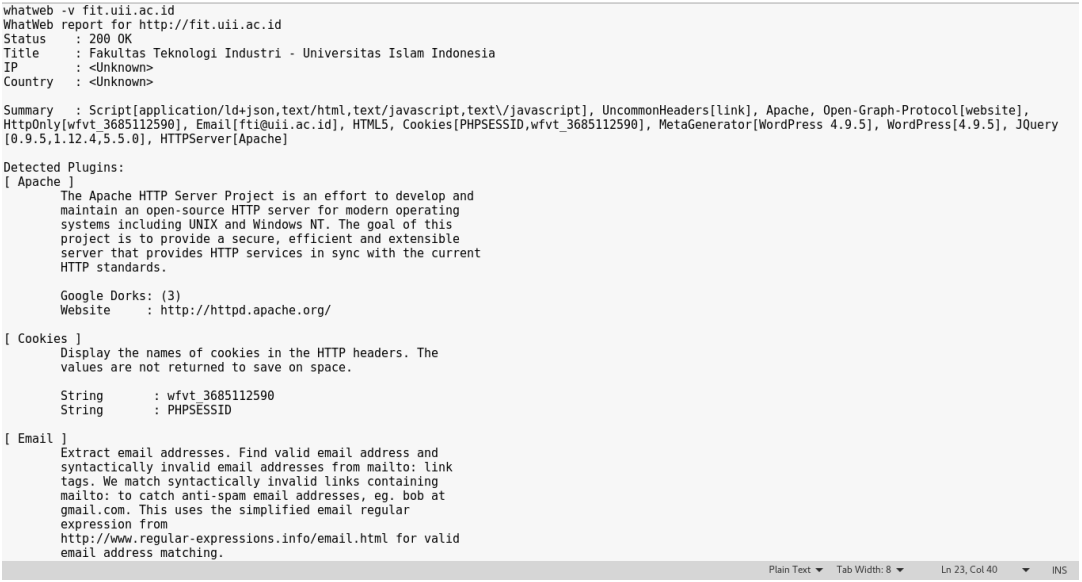
Gambar 4. 28 OS Fingerprinting dengan zenmap

Tahap selanjutnya adalah *service fingerprinting* untuk mengetahui layanan yang ada pada *port* yang terbuka dengan lebih jelas. *Tools* yang digunakan adalah nmap dari hasil menggunakan nmap didapatkan informasi antara lain jenis *web server* yang digunakan yaitu Apache httpd versi SSH yaitu OpenSSH 5.3 (protocol 2.0) dan informasi lain seperti pada Gambar 4. 29.

```
root@kali:~# nmap -sS -sV fit.uii.ac.id

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-24 22:33 WIB
Nmap scan report for fit.uii.ac.id (103.220.113.21)
Host is up (0.014s latency).
rDNS record for 103.220.113.21: cpanel-node02.uii.ac.id
Not shown: 989 filtered ports
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        Pure-FTPd
22/tcp   open   ssh        OpenSSH 5.3 (protocol 2.0)
53/tcp   closed domain
80/tcp   open   http       Apache httpd
110/tcp  open   pop3       Dovecot pop3d
143/tcp  open   imap       Dovecot imapd
443/tcp  open   ssl/ssl    Apache httpd (SSL-only mode)
587/tcp  open   smtp       Exim smtpd 4.89
993/tcp  open   ssl/imap   Dovecot imapd
995/tcp  open   ssl/pop3   Dovecot pop3d
8080/tcp closed http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.50 seconds
```

Gambar 4. 29 Service fingerprinting dengan nmap

Kemudian untuk mengumpulkan informasi lebih banyak lagi digunakan aplikasi whatweb. Dari hasil aplikasi whatweb memberikan informasi seperti pada Gambar 4. 30. Hasil dari whatweb menunjukan bahwa HTTP *server* yang digunakan adalah Apache dan juga menunjukan bahwa *web* fit.uii.ac.id menggunakan Wordpress versi 4.9.5. Dan pada tahap ini didapatkan informasi penting yang dapat digunakan untuk tahap selanjutnya antara lain *port* dan jenis layanan pada *server*.



```
whatweb -v fit.uii.ac.id
WhatWeb report for http://fit.uii.ac.id
Status    : 200 OK
Title     : Fakultas Teknologi Industri - Universitas Islam Indonesia
IP        : <Unknown>
Country   : <Unknown>

Summary   : Script[application/ld+json,text/html,text/javascript,text\/javascript], UncommonHeaders[link], Apache, Open-Graph-Protocol[website],
HttpOnly[wfvt_3685112590], Email[fti@uii.ac.id], HTML5, Cookies[PHPSESSID,wfvt_3685112590], MetaGenerator[WordPress 4.9.5], WordPress[4.9.5], JQuery
[0.9.5,1.12.4,5.5.0], HTTPServer[Apache]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : wfvt_3685112590
        String       : PHPSESSID

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.
```

Plain Text Tab Width: 8 Ln 23, Col 40 INS

Gambar 4. 30 Hasil dari whatweb

Proses di atas juga diterapkan untuk pengujian pada semua *web* target yang sudah dibagi menjadi 3 alamat IP *server* yang ada pada Tabel 4. 6 sebelumnya sehingga didapatkan hasil seperti pada Tabel 4. 7 , Tabel 4. 8, dan Tabel 4. 9 di bawah ini

Tabel 4. 7 Hasil pencarian informasi

Host IP	103.220.113.21		
Domain name	www.fit.uii.ac.id		
Sistem operasi	Linux 2.6.32 (92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	Pure-FTPd
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Tabel 4. 8 Hasil pencarian informasi

Host IP	103.220.113.20		
Domain name	www.law.uii.ac.id		
Sistem operasi	Linux 2.6.32 (Kemungkinan 92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	Pure-FTPd
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Tabel 4. 9 Hasil pencarian informasi

Host IP	103.220.113.24		
Domain name	www.fcep.uii.ac.id		
Sistem operasi	Linux 2.6.32 (92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	ProFTPD 1.3.5b
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Tahap selanjutnya adalah *vulnerability indentification* dimana akan dimulai mencari celah keamanan yang ada pada sistem dan *server* dari 10 target yang ada berdasarkan informasi yang diperoleh sebelumnya secara manual dan dengan menggunakan *automated vulnerability scanner* yaitu WPScan dan *tools* otomatisasi OWASPZap yang dikembangkan penulis guna mempermudah dalam melakukan pencarian *vulnerability* target. Pada tahap sebelumnya telah diperoleh informasi bahwa *server* target dimungkinkan menggunakan sistem operasi Linux 2.6.32 berdasarkan informasi yang didapat sistem operasi Linux 2.6.32 memiliki beberapa kelemahan dan diantaranya memiliki nilai *Common Vulnerability Scoring System* (CVSS) sembilan atau lebih tinggi seperti yang terangkum dalam Tabel 4. 10 yang bersumber dari salah satu database CVSS yaitu cvedetails.com (https://www. cvedetails.com)

Tabel 4. 10 Celah keamanan pada linux 2.6.32 menurut cvedetails.com

CVE ID	**Jenis kelemahan**	**Akses yang didapatkan**	**Auntentikasi**	**Confindentiality**	**Integrity**	**Availability**
CVE-2010-2495	DoS	Tidak ada	Tidak perlu	Complete	Complete	Complete
CVE-2009-4538	DoS	Tidak ada	Tidak perlu	Complete	Complete	Complete

Dari tabel tersebut dapat dilihat bahwa jenis kelemahan yang terdapat pada sistem operasi Linux 2.6.32 adalah *Denial of Service* (DoS) yang dapat mengakibatkan terganggunya aspek-aspek keamanan informasi yaitu confidentiality,integrity, dan availibility. Untuk melakukan ekseskusi terhadap kelemahan yang terdapat pada Linux 2.6.32 juga tidak memerlukan auntentikasi administrator atau root cukup akses user biasa pada terminal *server* dan dapat mengeksekusi serangan.

Sementara itu dari informasi sebelumnya diketahui bahwa *web* target rata-rata berbasis *WordPress* di sini *web* yang diuji adalah www.fpscs.uii.ac.id sehingga di sini penulis menggunakan aplikasi WPScan untuk melakukan *vulnerability indentification*. Dari hasil *scanning* ditemukan kemungkinan terdapat celah kemanan seperti ditunjukan pada Tabel 4. 11 di bawah ini.

Tabel 4. 11 Hasil *vulnerability identification* WPScan.

Jenis ancaman	**Jumlah**
Directory listing	6
Path Traversal	1
Structure & Information Disclosure	1

Dari hasil *scanning* ini juga didapatkan hasil yang dicurigai sebagai *username login* admin seperti Gambar 4. 31

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+-----------+-----------+
    | Id | Login     | Name      |
    +----+-----------+-----------+
    | 1  | fpsb-uii  | fpsb uii  |
    | 2  | webmaster | webmaster |
    +----+-----------+-----------+
```

Gambar 4. 31 Username login

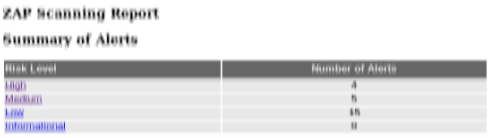
Di sini penulis melakukan 2kali *scanning* menggunakan *tools* WPScan pada tanggal yang berbeda dan mendapatkan hasil yang sedikit berbeda seperti ditunjukan pada Tabel 4. 12

Tabel 4. 12 Perbedaan hasil WPScan

Hasil *scanning* pertama	Hasil *scanning* kedua
[+] WordPress version 4.8.2 (Released on 2017-09-19) identified from advanced fingerprinting, meta generator, links opml, stylesheets numbers [!] 1 vulnerability identified from the version number [!] Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset Reference: https://wpvulndb.com/vulnerabilities/8807 Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html Reference: https://core.trac.wordpress.org/ticket/25239 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295 [+] Enumerating installed plugins (only ones marked as popular) ... Plain Text Tab Width: 8 Ln 23, Col 93 INS	[+] WordPress version 4.8.6 (Released on 2018-04-03) identified from meta generator, links opml [+] Enumerating installed plugins (only ones marked as popular) ... Time: 00:06:57 <==========> (1496 / 1496) 100.00% Time: 00:06:57 [+] We found 8 plugins: [+] Name: 404-to-301 - v2.3.3 Latest version: 2.3.3 (up to date) Plain Text Tab Width: 8 Ln 22, Col 86 INS

Dari hasil yang ditunjukan Tabel 4. 12 terdapat perbedaan dari versi Wordpress pada proses *scanning* pertaman dan kedua. Pada hasil pertama *web* www.fpscs.uii.ac.id masih menggunaka Wordpress versi 4.8.2 yang dimana dari hasil *scanning* menggunakan *tools* WPScan terdapat kemungkinan celah keamanan yaitu *Host Header Injection in Password Reset*. Kemudian pada *scanning* kedua Wordpress sudah diperbaruai menjadi versi 4.8.6 di sini dapat disimpulkan bahwa admin cukup tanggap dalam mengelola *website* karena melakukan *update* secara berkala.

Selanjut dari hasil *scanning* menggunakan *tools* otomatisasi OWASPZap yang dikembangkan menunjukan terdapat 24 jenis kemungkinan ancaman dengan 4 kategori memiliki tingkat ancaman *High*, 5 kategori memiliki tingkat ancaman *Medium*, 15 kategori lainya memiliki tingkat ancaman *Low* dan 0 *Informational* seperti pada Gambar 4. 32 di bawah ini dan jenis-jenis kemungkinan ancaman dari hasil *scanning* terdapat dalam Tabel 4. 13.


ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	5
Low	15
Informational	0

Gambar 4. 32 Contoh kategori tingkat keamanan low.

Tabel 4. 13 Kategori ancaman hasil proses *scan* menggunakan *tools* otomatisasi OWASPZap

Tingkat Ancaman	**Jenis Ancaman**	**Jumlah**
HIGH	Path Traversal	1
HIGH	Cross Site Scripting (Reflected)	1
HIGH	SQL Injection	1
HIGH	Remote OS Command Injection	1
MEDIUM	X-Frame-Options Header Not Set	3
MEDIUM	Application Error Disclosure	1
MEDIUM	Secure Pages Include Mixed Content (Including Scripts)	1
LOW	X-Content-Type-Options Header Missing	2
LOW	Cookie No HttpOnly Flag	4
LOW	Cross-Domain JavaScript Source File Inclusion	3
LOW	Password Autocomplete in Browser	2
LOW	Web Browser XSS Protection Not Enabled	1
LOW	Secure Pages Include Mixed Content	1
LOW	Incomplete or No Cache-control and Pragma HTTP Header Set	1
LOW	Cookie Without Secure Flag	1

Dan hasil seluruh *scanning* terhadap semua target dengan menggunakan langkah yang sama seperti dijelaskan sebelumnya dapat dilihat pada Tabel 4. 14 di bawah ini

Tabel 4. 14 Versi WordPress hasil *scanning* menggunakan *tools* WPScan

URL	**Sebelum**	**Sesudah**
www.fcep.uii.ac.id	WordPress version 4.8.1	WordPress version 4.9.5
www.fis.uii.ac.id	WordPress version 4.4.11	WordPress version 4.9.5
www.fit.uii.ac.id	WordPress version 4.4.11	WordPress version 4.9.5
www.law.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.science.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.dpka.uii.ac.id	WordPress version 4.4.11	WordPress version 4.4.15
www.itsupport.uii.ac.id	WordPress version 4.8.2	WordPress version 4.8.6
www.bpm.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.humas.uii.ac.id	-	-

Tabel 4. 14 menunjukan hasil *scanning* menggunakan *tools* WPScan terhadap versi Wordpress dari semua target karena rata-rata bertipe Wordpress dari hasil tersebut menunjukan bahwa admin tanggap dalam mengelola karena telah melakukan *update* secara berkala terhadap versi Wordpress sebelumnya dan pada *URL* www.humas.uii.ac.id tidak mendapatkan hasil dari *tools* WPScan karena *web* tidak bertipe Wordpress melainkan menggunakan JavaScript.

Selanjut pada Tabel 4. 15 akan dijelaskan hasil *scanning* menggunakan aplikasi WPScan terhadap semua target akan kemungkinan terdapat celah keamanan

Tabel 4. 15 Hasil *scanning* menggunakan aplikasi WPScan.

URL	**Jenis ancaman**	**Jumlah**	**Kemungkinan user login**
www.fcep.uii.ac.id	Directory listing	7	Tidak ditemukan
	Information Disclosure	1	
	SQL Injection	1	
	Path Traversal	1	
	Cross-Site Scripting (XSS)	1	
	Host Header Injection in Password Reset	1	
www.fis.uii.ac.id	Directory listing	10	Ditemuka
	Cross-Site Scripting (XSS)	1	
	Host Header Injection in Password Reset	1	
www.fit.uii.ac.id	Directory listing	7	Tidak Ditemukan
	Remote Path Traversal File Access	1	
	Style Editing CSRF	1	

URL	Jenis ancaman	Jumlah	Kemungkinan user login
	Authenticated Stored XSS & SQL Injection	1	
	Information Disclosure	1	
	Host Header Injection in Password Reset	1	
www.law.uii.ac.id	Directory listing	10	Tidak Ditemukan
	Host Header Injection in Password Reset	1	
	Style Editing CSRF	3	
	Remote Path Traversal File Access	1	
	Cross-Site Scripting (XSS)	8	
	SQL Injection	4	
	Multiple vulnerabilities in login CAPTCHA	1	
	information Disclosure	1	
	File Upload Remote Code Execution	1	
www.science.uii.ac.id	Cross-Site Scripting (XSS)	1	Ditemuka
	Directory listing	2	
	information Disclosure	1	
	Host Header Injection in Password Reset	1	
www.dpka.uii.ac.id	Cross-Site Scripting (XSS)	2	Ditemuka
	Host Header Injection in Password Reset	1	
	Revolution Local File Disclosure	1	
	Revolution Shell Upload	1	
	Directory listing	4	
www.itsupport.uii.ac.id	Directory listing	11	Ditemukan
	Host Header Injection in Password Reset	1	
	Cross-Site Scripting (XSS)	1	
	Authenticated PHP Object Injection	1	
www.bpm.uii.ac.id	Cross-Site Scripting (XSS)	3	Ditemukan
	Directory listing	6	
	Host Header Injection in Password Reset	1	
	CSRF	3	
	Authenticated Multisite Remote Code Execution	1	
	Information Disclosure	1	
	Missing Settings Authorization	1	

URL	Jenis ancaman	Jumlah	Kemungkinan user login
	Revolution Local File Disclosure	1	
	Revolution Shell Upload	1	
	Open Redirect	1	
www.humas.uii.ac.id	-	-	-

Dari hasil *scanning* menggunakan WPScan pada Tabel 4. 15 hanya www.humas.uii.ac.id yang tidak terdapat hasil *scannig* dikarenakan *web* www.humas.uii.ac.id tidak bertipe Wordpress seperti yang sudah dijelaskan sebelumnya. Selanjutnya hasil dari *scanning* menggunakan *tools* otomatisasi OWASPZap yang dikembangkan terdapat pada Tabel 4. 16 di bawah ini.

Tabel 4. 16 Hasil *scan* menggunakan *tools* otomatisasi OWASPZap

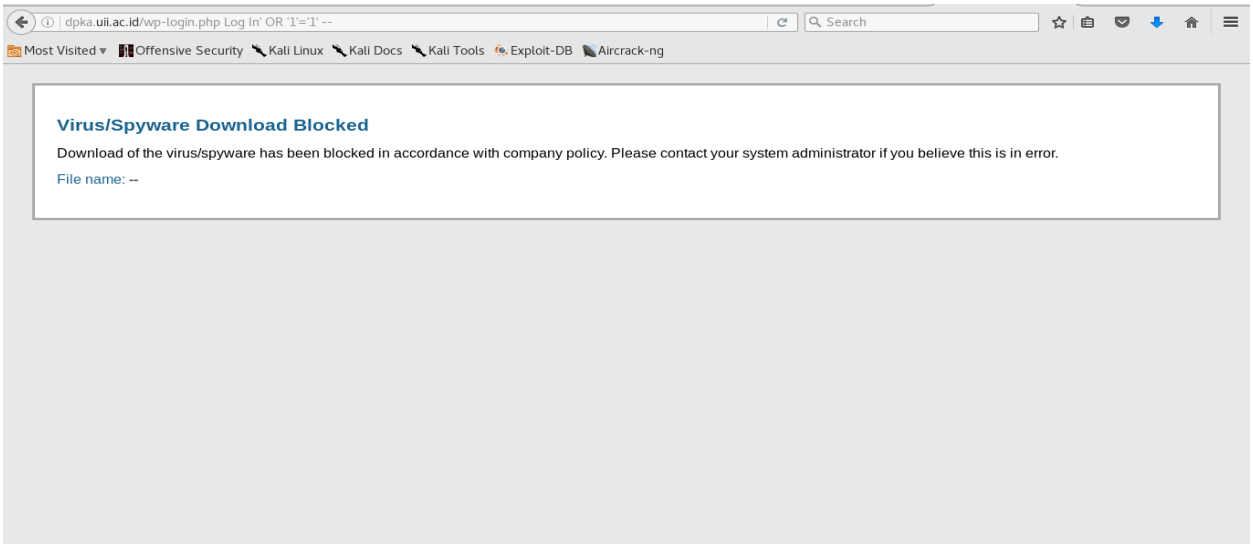
URL	Tingkat Ancaman	Jenis Ancaman	jumlah
www.fcep.uii.ac.id	HIGH	Path Traversal	1
	MEDIUM	X-Frame-Options Header Not Set	2
	MEDIUM	Application Error Disclosure	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	2
	LOW	Cross-Domain JavaScript Source File Inclusion	1
www.fis.uii.ac.id	MEDIUM	X-Frame-Options Header Not Set	6
	MEDIUM	Application Error Disclosure	1
	LOW	Web Browser XSS Protection Not Enabled	4
	LOW	Cookie No HttpOnly Flag	4
	LOW	X-Content-Type-Options Header Missing	10
	LOW	Content-Type Header Missing	2
	LOW	Cross-Domain JavaScript Source File Inclusion	4
	LOW	Private IP Disclosure	1
www.fit.uii.ac.id	HIGH	Cross Site Scripting (Reflected)	1
	HIGH	Remote OS Command Injection	1
	HIGH	Path Traversal	1
	HIGH	SQL Injection	1

URL	Tingkat Ancaman	Jenis Ancaman	jumlah
	MEDIUM	X-Frame-Options Header Not Set	2
	MEDIUM	Directory Browsing	1
	MEDIUM	Application Error Disclosure	2
	MEDIUM	Format String Error	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	2
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie Without Secure Flag	1
	LOW	Incomplete or No Cache-control and Pragma HTTP Header Set	1
	LOW	Secure Pages Include Mixed Content	1
www.law.uii.ac.id	HIGH	Remote OS Command Injection	1
	HIGH	SQL Injection	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	X-Content-Type-Options Header Missing	1
	LOW	Cookie No HttpOnly Flag	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Web Browser XSS Protection Not Enabled	1
	LOW	Password Autocomplete in Browser	1
www.science.uii.ac.id	HIGH	Path Traversal	1
	HIGH	Remote OS Command Injection	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Application Error Disclosure	1
	MEDIUM	Format String Error	1
	LOW	Cookie No HttpOnly Flag	1
	LOW	Private IP Disclosure	1
	LOW	Password Autocomplete in Browser	1
www.dpka.uii.ac.id	HIGH	SQL Injection	1
	HIGH	Remote OS Command Injection	1
	HIGH	Path Traversal	1

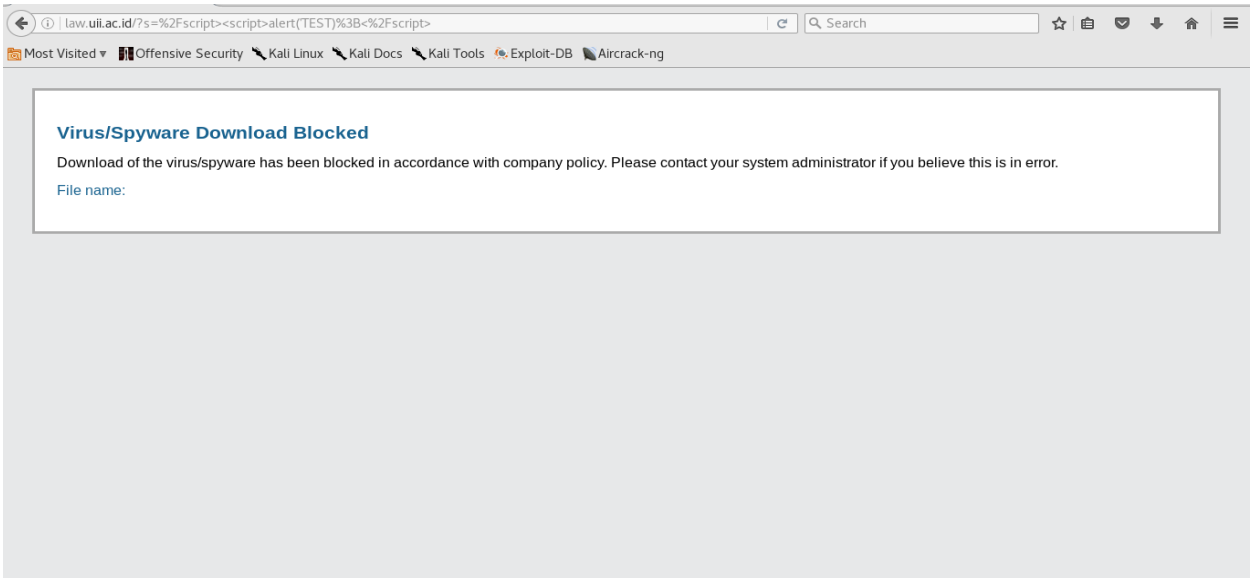
URL	Tingkat Ancaman	Jenis Ancaman	jumlah
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
www.itsupport.uii.ac.id	HIGH	Remote OS Command Injection	
	HIGH	Remote File Inclusion	
	HIGH	Path Traversal	
	HIGH	SQL Injection	
	MEDIUM	Application Error Disclosure	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	1
	LOW	Private IP Disclosure	1
	LOW	X-Content-Type-Options Header Missing	1
www.bpm.uii.ac.id	HIGH	Path Traversal	1
	HIGH	Remote OS Command Injection	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Password Autocomplete in Browser	1
	LOW	Cookie No HttpOnly Flag	1
www.humas.uii.ac.id	HIGH	SQL Injection	1
	MEDIUM	Directory Browsing	1
	MEDIUM	X-Frame-Options Header Not Set	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie No HttpOnly Flag	1

Dengan melakukan analisis terhadap semua kemungkinan celah keamanan yang ditemukan terhadap semua *web* target yang memiliki domain uii.ac.id didapatkan hasil terdapat beberapa *false positive* dari hasil *scanning* celah keamanan *false positive* sendiri terjadi

dikarenakan aplikasi *vulnerability scanner* mendeteksi query yang mirip dengan query pada celah keamanan tertentu sehingga setelah dilakukan pengujian secara manual tidak terjadi efek tertentu terhadap *web* target. Dan juga serangan terhadap celah keamanan terhalang oleh *firewall* yang dimiliki oleh *web* target seperti ditunjukan pada Gambar 4. 33 dan Gambar 4. 34.



Gambar 4. 33 Pengujian terhadap celah keamanan *sql injection.*



Gambar 4. 34 Pengujian terhadap celah keamanan XSS

Pada Gambar 4. 33 dan Gambar 4. 34 penguji melakukan serangan Sqli Injection dan XSS yang sebelumnya terdeteksi sebagai kemungkinan celah keamanan menggunakan *browser* secara manual akan tetapi terhalang oleh *firewall* yang dimiliki oleh *web* target.

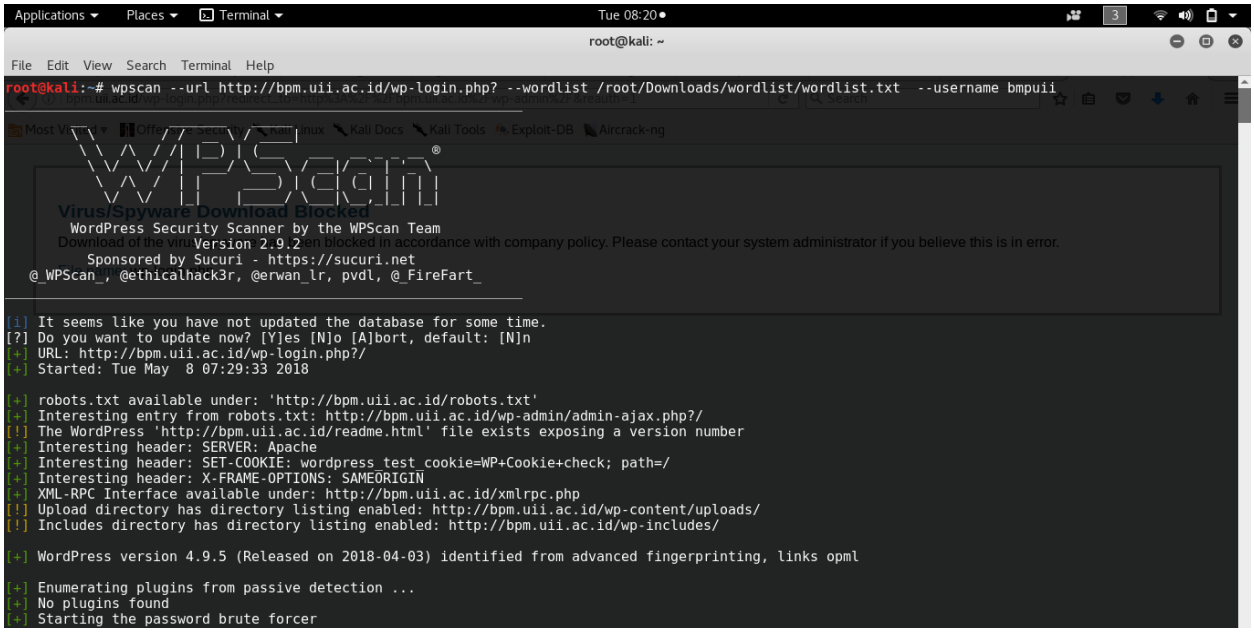
Selanjut penulis mencoba melakukan *scanning* menggunakan Whatwaf untuk mencari tau *firewall* apa saja yang terdapat pada *web* target. Dari hasil *scanning* terdapat beberapa *firewall* yang terdeteksi pada *web* target yang antara lain dapat dilihat pada Tabel 4. 17 di bawah ini.

Tabel 4. 17 Daftar nama *firewall* yang terdeteksi aplikasi WhatWaf

URL	Firewall
www.fis.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fit.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fpscs.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.law.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.bpm.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.science.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fcep.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.dpka.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.humas.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.itsupport.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection

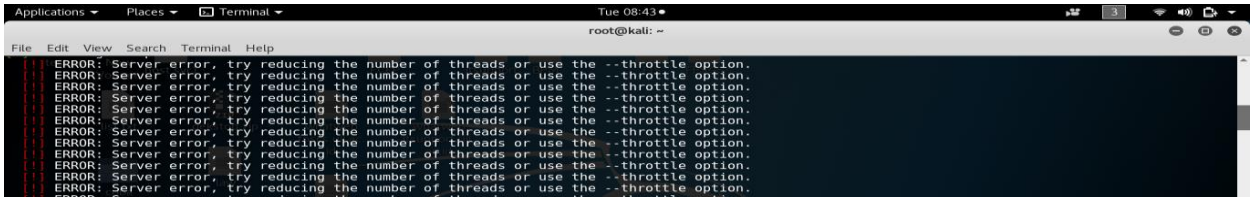
Selanjutnya penulis melakukan pengujian terhadap kemungkinan *user login* yang ditemukan pada tahap sebelumnya menggunakan aplikasi WPScan dengan metode *brute force*

yang berjenis *dictionary attack* dengan menggunakan *user login* yang sudah ditemukan sebelumnya dan untuk mencari password menggunakan *dictionary password* yang terdapat pada Kali linux yang memiliki jumlah kata sekitar 13 juta. Serangan dilakukan terhadap halaman form login *web* target di sini penulis melakukan pengujian terhadap www.bpm.uii.ac.id seperti pada Gambar 4. 35 di bawah ini



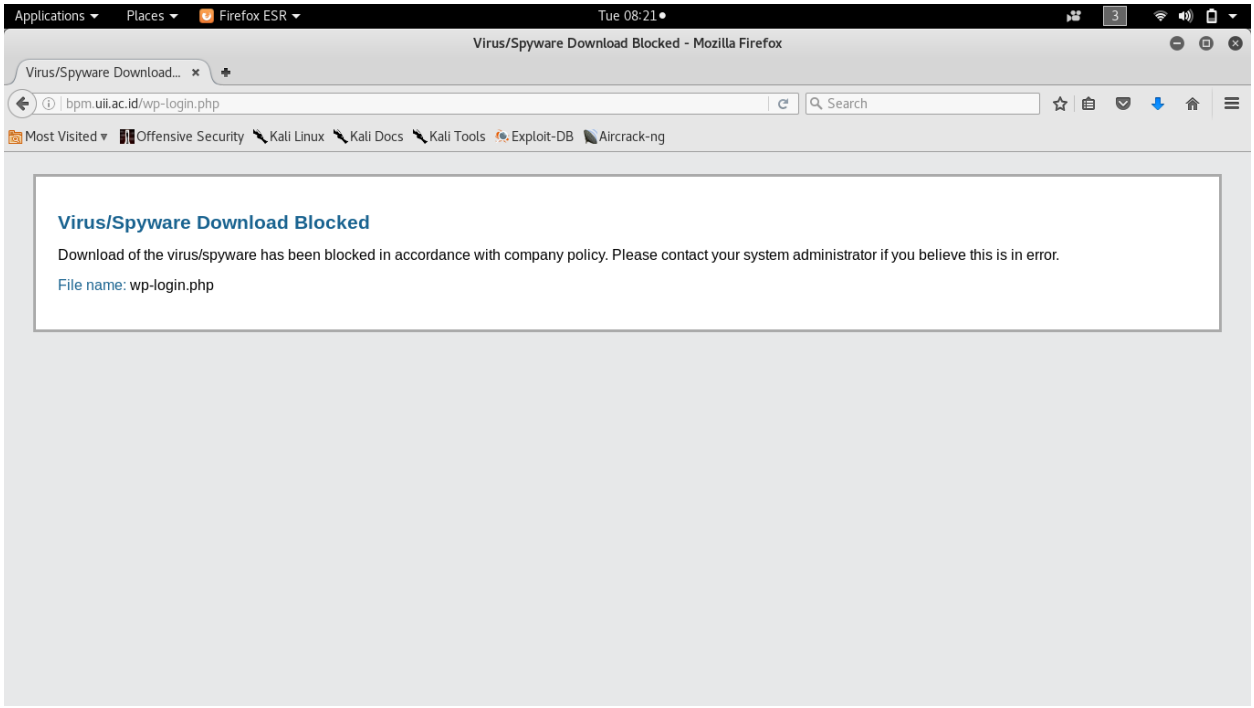
Gambar 4. 35 Serangan *brute force* dengan WPScan

Hasil serangan *brute force* menggunakan aplikasi WPScan dinyatakan tidak berhasil dikarenakan langsung terjadi notification *server eror* seperti pada Gambar 4. 36 yang kemungkinan besar serangan yang dilakukan langsung terhalang oleh *firewal*l yang dimiliki oleh *web* target.



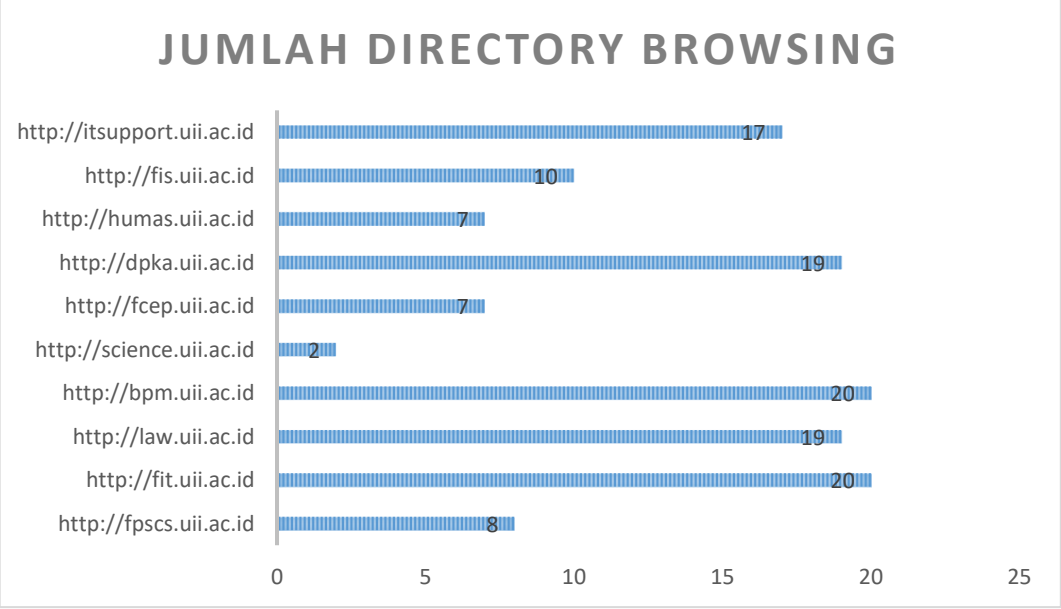
Gambar 4. 36 Hasil serangan *brute force* dengan WPScan

Kemungkinan serangan terhalang oleh *firewall* yang dimiliki oleh *web* target dikuatkan dengan penulis yang mencoba melakukan akses menggunakan *browser* ke halaman login *web* target dan terdapat peringatan seperti yang ditunjukan pada Gambar 4. 37 di bawah ini.



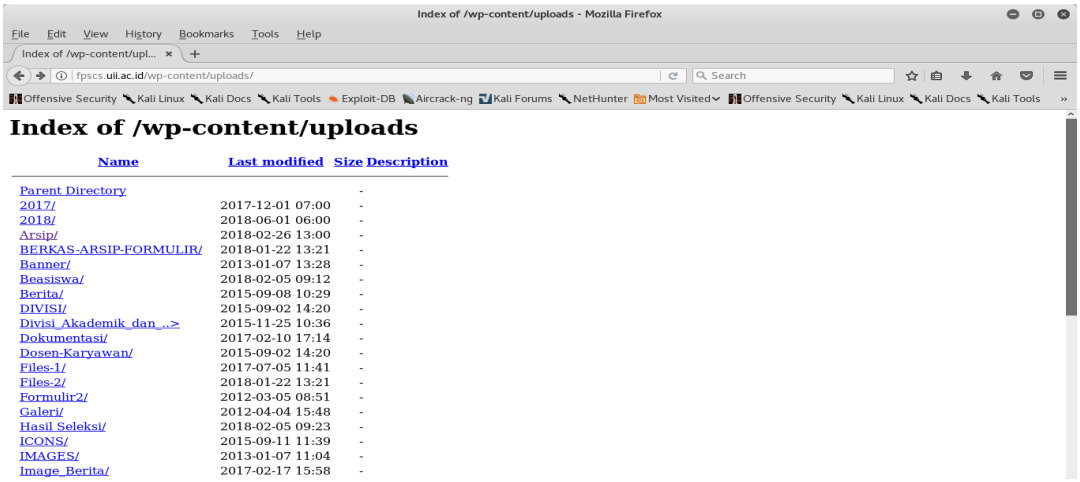
Gambar 4. 37 Akses halaman login *web* target.

Selama proses *brute force* dijalankan semua akses ke halaman login *web* taget yang menggunakan *gateway* yang sama tidak dapat dilakukan dan akan otomatis muncul peringatan seperti Gambar 4. 37 di atas. Setelah proses *brute force* dihentikan dan menunggu kurang lebih 5 menit halaman login dapat diakses secara normal kembali.



Gambar 4. 38 Jumlah directory browsing pada web target.

di atas menunjukan jumlah *directory browsing* pada *web* target yang dapat diakses oleh user tanpa ijin admin sehingga didapatkan beberapa informasi tentang *directory* yang terdapat dalam *web* target seperti ditunjukan Gambar 4. 38



Gambar 4. 39 Directory browsing pada *URL* www.fpscs.uii.ac.id

Gambar menunjukan bahwa *directory* pada alamat *URL* www.fpscs.uii.ac.id/wp-content/upload dapat di akses oleh sembarang user tanpa memerlukan ijin admin sehingga didapatkan informasi file apa saja yang pernah diunggah oleh admin *web* www.fpscs.uii.ac.id.

4.4 Analisis

Dari hasil *scanning* yang telah dilakukan pada proses sebelumnya ditemukan bahwa 10 *web* target telah menggunakan CPanel dan terdapat beberapa celah keamanan yang dapat membahayakan keamanan *web* yang dikelola oleh UII sehingga perlu segera dilakukan tindakan pencegahaan lebih dini dan rata-rata kemungkinan celah keamanan yang ditemukan pada hasil *scanning* menggunakan aplikasi WPScan dan otomatisasi OWASPZap terdeteksi pada *plugin* yang terdapat dalam *web*. Kebanyakan *plugin* belum dilakukan pembaruan oleh pengelola sehingga terdapat *query* tertentu yang terindikasi sebagai celah keamanan oleh aplikasi *scanning* akan tetapi 10 *web* target yang memiliki domain uii.ac.id tertolong dengan *firewall* yang di miliki karena serangan yang dilakukan terhadap celah keamanan yang ditemukan terhalang dan dapat langsung di cegah oleh *firewall*. Dari hasil *scanning* menggunakan WPScan dan otomatisasi OWASPZap juga terdapat *false positive* dimana peringatan keamanan yang ditemukan tidak terbukti atau palsu hal ini terjadi karena aplikasi mendeteksi *query* yang mungkin menjadi ciri-ciri dari sebuah celah keamanan sehingga

aplikasi memberikan peringatan. Selain itu juga perlu dilakukan konfigurasi kembali terhadap pengaturan *server* yang dimiliki 10 *web* target karena terdapat celah keamanan yang cukup sensitif. Dari semua proses yang telah dilakukan pada tahap sebelumnya penulis memiliki beberapa rekomendasi antara lain

Tabel 4. 18 Solusi dari celah keamanan yang ditemukan.

Celah keamanan	**Solusi**
Open DNS *Server*	Melakukan konfigurasi kembali pada DNS *server* agar mengijinkan IP addres yang sudah ditentukan saja yang dapat melaukan permintaan zone transfer
Sensitive Data Exposure	Melakukan pengamanan dengan melakukan *encryption* pada data penting seperti userlogin
Directory Browsing	Melakukan disable directori browsing melalui CPanel atau dapat melakukan pemblokiran menggunakan file .htacces

BAB V
KESIMPULAN

5.1 Kesimpulan

Dalam melakukan uji *penetration testing* menggunakan metode OWASP10 tahun 2013 yang bertujuan untuk menguji tingkat keamanan pada sistem 10 *web* yang berdomain uii.ac.id yang di miliki oleh Universitas Isalam Indonesia berdasarkan dari seluruh kegiatan yang dilakukan maka dapat diambil beberapa kesimpulan yang antara lain sebagai berikut:

a. Metode OWASP10 tahun 2013 masih sangat cocok dijadikan sebagai dasar dalam melakukan uji *penetration testing* pada 10 *web* yang berdomain uii.ac.id. Karena masih ditemukan beberapa celah keamanan yang sesuai dengan daftar OWASP10 tahun 2013
b. Berhasil dikembangkan aplikasi otomatisasi OWASPZap yang bertujuan untuk memudahkan dalam melakukan uji *penetration* menggunakan metode OWASP
c. Keamanan sistem pada 10 *web* target yang memiliki domain uii.ac.id masih belum memenuhi prinsip keamanan CIA TRIAD yaitu *confidentiality*. Hal tersebut dapat dilihat dari beberapa keberhasilan eksploitasi celah keamanan yang ada sehingga didapatkan informasi penting yang seharusnya memiliki hak akses khusus.
d. Domain uii.ac.id memiliki *firewall* yang cukup bisa diandalkan dalam menanggulangi serangan-serangan yang tidak bertanggung jawab.

5.2 Saran

Berdasarkan penelitian yang sudah dilakukan terdapat beberapa saran yang dapat diterapkan pada penelitian berikutnya dan juga untuk sistem dan jaringan pada Universitas Islam Indonesia sebagai objek penelitian. Dan terdapat beberapa kekurangan pada pengembangan otomatisasi OWASPZap yang dapat dikembangkan lebih lanjut pada peneletian berikutnya yang antara lain:

a. Perlunya dilakukan pengujian pada seluruh sistem yang memiliki domain uii.ac.id agar segera dapat ditanggulangi jika terdapat kebocoran celah keamanan.
b. Melakukan konfigurasi kembali pada *server* uii.ac.id agar hanya sebagian orang tertentu saja yang dapat melakukan *request* terhadap data yang sensitif.
c. Perlu dilakukan *update* secara berkala terhadap beberapa *plugin* yang terdapat dalam *web* yang dikelola.

d. Melakukan konfigurasi kembali terhadap sistem *web* agar data yang seharusnya tidak dapat ditampilkan bisa ditampilkan.
e. Perlu dilakukan *encryption* terhadap data yang penting untuk mengurangi resiko terjadinya kebocoran informasi yang penting.
f. Masih kurangnya kesadaran pengelola untuk selalu rutin melakukan pembaruan pada sistem mereka untuk mengurangi resiko adanya celah keamanan.

DAFTAR PUSTAKA

Abidin. (2015). Penetration Testing Menggunakan Metode Owasp (Open Web Application Security Project). *Ali Zainal Abidin*.

Dirgahayu. (et.all, 2015). Penerapan Metode ISSAF dan OWASP versi 4 untuk Uji Kerentanan Web Server. *Dr. Raden Teduh Dirgahayu, ST., M.Sc. , Yudi Prayudi S.Si.,M.Kom.,Adi Fajaryanto*.

Handisonj. (2013). Diambil kembali dari https://handisonj.wordpress.com: https://handisonj.wordpress.com/2013/09/16/cia-confidentiality-integrity-availability/

Harvester, T. (2014). Diambil kembali dari https://tools.kali.org/information-gathering/theharvester

Herfiedhantya. (2014). *UJI PENETRASI SISTEM KEAMANAN JARINGAN UNIVERSITAS GADJAH MADA DENGAN INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK (ISSAF).* Yogyakarta.

Isparmo. (2016). Diambil kembali dari http://isparmo.web.id: http://isparmo.web.id/2016/11/21/data-statistik-pengguna-internet-indonesia-2016/

learn-penetration-testing. (t.thn.). Diambil kembali dari www.guru99.com: https://www.guru99.com/learn-penetration-testing.html

Masscan. (2017). Diambil kembali dari https://www.freakzsec.net/2017/11/masscan-mempercepat-scan-port-tcp.html?m=1

Nmap. (t.thn.). Diambil kembali dari https://nmap.org/man/id/index.html

OWASP. (2011). Diambil kembali dari http://infokomq.blogspot.co.id/2011/01/owasp-sekuritas-komputer.html

Owaspzap. (2016). Diambil kembali dari https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Pseudocode. (2017). Diambil kembali dari https://herlansaputra.wordpress.com/2017/10/25/pengertian-algoritma-flowchart-pseudocode-ipo-progam-bahasa-pemograman/

Whitman. (July 2007). *Principles of Incident Response and Disaster Recovery.*

Wpscan. (2014). Diambil kembali dari https://scriptkiddiew.wordpress.com/2014/06/08/wpscan/ & http://anher323.blogspot.co.id/2016/01/cek-celah-vulnerability-cms-wordpress.html

LAMPIRAN

A. Report
B. Hasil *scanning* dengan WPScan
C. Hasil *scanning* dengan Otomatisasi OWASPzap
D. Hasil *scanning port*

REPORT

PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10

Disusun Oleh:

N a m a : Adetya Putra Dewanto

NIM : 13523025

Yogyakarta , 13 Agustus 2018

Target :

Web yang memiliki domain uii.ac.id yang akan di uji terbagi menjadi 3 yaitu 6 *web* Fakultas, 2 Direktorat, dan 2 Badan usaha yang dimiliki oleh Universitas Islam Indonesia yang dipilih secara acak. Daftar *web* yang akan diuji dapat dilihat pada Table 1.

Table 1 Target *penetration testing*

NO	FAKULTAS	Direktorat	Badan
1	www.fcep.uii.ac.id	www.dpka.uii.ac.id	www.itsupport.uii.ac.id
2	www.fis.uii.ac.id	www.humas.uii.ac.id	www.bpm.uii.ac.id
3	www.fit.uii.ac.id		
4	www.fpscs.uii.ac.id		
5	www.law.uii.ac.id		
6	www.science.uii.ac.id		

Universitas Isalam Indonesia(UII) sebagai salah satu lembaga pendidikan perguruan tinggi swasta terkemuka di Indonesia memanfaatkan jaringan internet yaitu *web* sebagai media dalam menyampaikan informasi kepada pihak luar dan menghubungkan sivitas sivitas yang ada guna memudahkan dalam penyampaian informasi. Proses *Penetration Testing (*Pentest*)* terhadapa 10 *web* yang berdomain uii.ac.id bertujuan untuk :

1. Apakah *web* yang dikelola oleh UII sudah memenuhi 3 aturan dasar keamana jaringan yaitu Confidentiality, Integrity, dan Availability
2. Menemukan celah keamanan pada sistem jika ada agar dapat segera dilakukan penanganan lebih dini

Metode yang digunakan dalam proses *Pentest* ini adalah OWASP10 tahun 2013 yang berisi 10 celah keamana yang sering ditemukan dalam *website* seperti yang ditunjukan pada Gambar 1 di bawah ini

OWASP TOP 10 – 2013
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

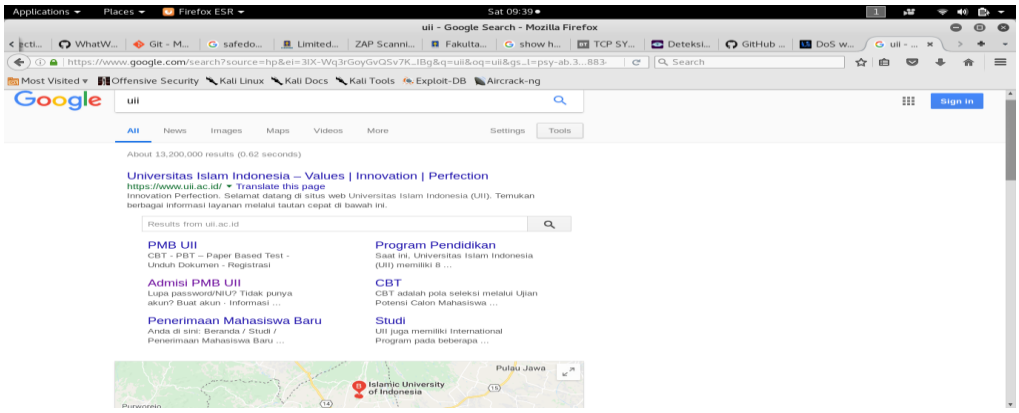
Gambar 1 OWASP 10 tahun 2013

Dalam proses *pentest* terhadap *web* yang berdomain uii.ac.id ini penguji disimulasikan sebagai penyerang dari luar yang sama sekali tidak mengetahui informasi tentang *web* yang dikelola oleh Universitas Islam Indonesia. Alur dalam melakukan proses *pentest* terdapat pada Gambar 2.

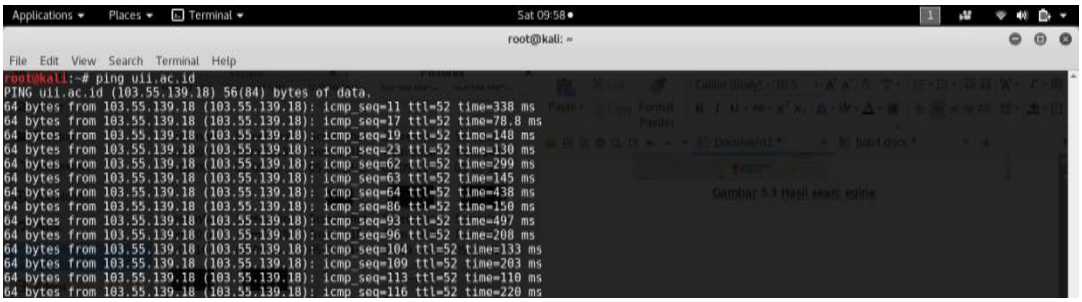
Gambar 2 Alur proses *penetration testing*

Footprinting

Pada tahap awal ini penulis menggunakan beberapa tools untuk mencari informasi tentang *web* target yang akan dilakukan uji pentest. Dengan menggunakan *search engine* yaitu google.com seperti terlihat pada Gambar 3 dimana penulis memasukan *keyword* uii. Pada Gambar 3 menunjukan google.com menampilkan hasil bahwa UII memiliki situs utaman yaitu https://www.uii.ac.id . Dengan menggunakan perintah ping seperti Gambar 4 didapatkan bahwa uii.ac.id memiliki IP address 103.55.139.18.



Gambar 3 Hasil *searc egine* google.com



Gambar 4 Hasil ping pada uii.ac.id

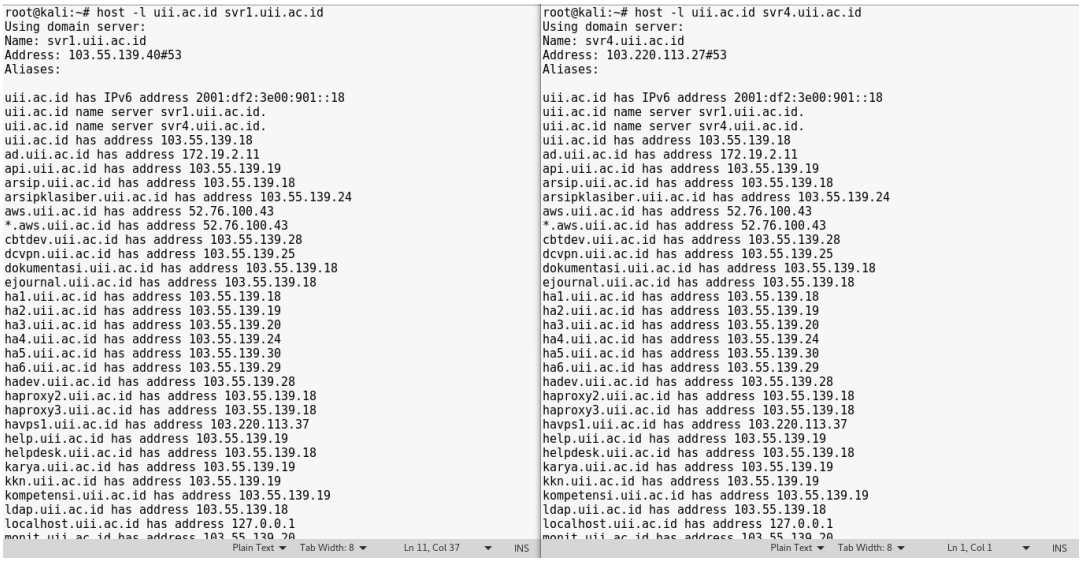
Selanjutnya menggunakan *tools* whois didapatkan hasil seperti pada Gambar 5 dimana terlihat bahwa uii.ac.id memiliki *block IP adders* dari 103.55.139.0 sampai dengan 103.55.139.255. Selain *block IP addres* juga didapatkan nama,email dan kontak pengelola server.

Gambar 5 Hasil whois

Dengan menggunakan perintah *host* didapatkan nameserver dari UII yaitu svr4.uii.ac.id, svr1.uii.ac.id dan juga didapatkan mail server yang bertanggung jawab untuk domain uii.ac.id yaitu seperti Gambar 6.

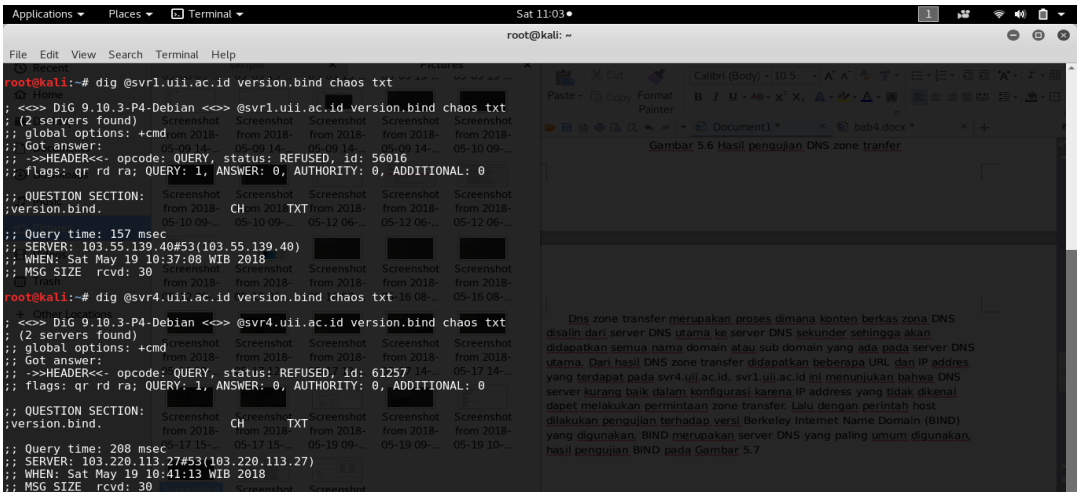
Gambar 6 Hasil host

Dari informasi yang didapatkan tersebut dilanjutkan dengan mencoba melakukan pengujian Domain Name Server (DNS) zone transfer untuk seluruh informasi dari uii.ac.id seperti Gambar 7 di bawah ini.



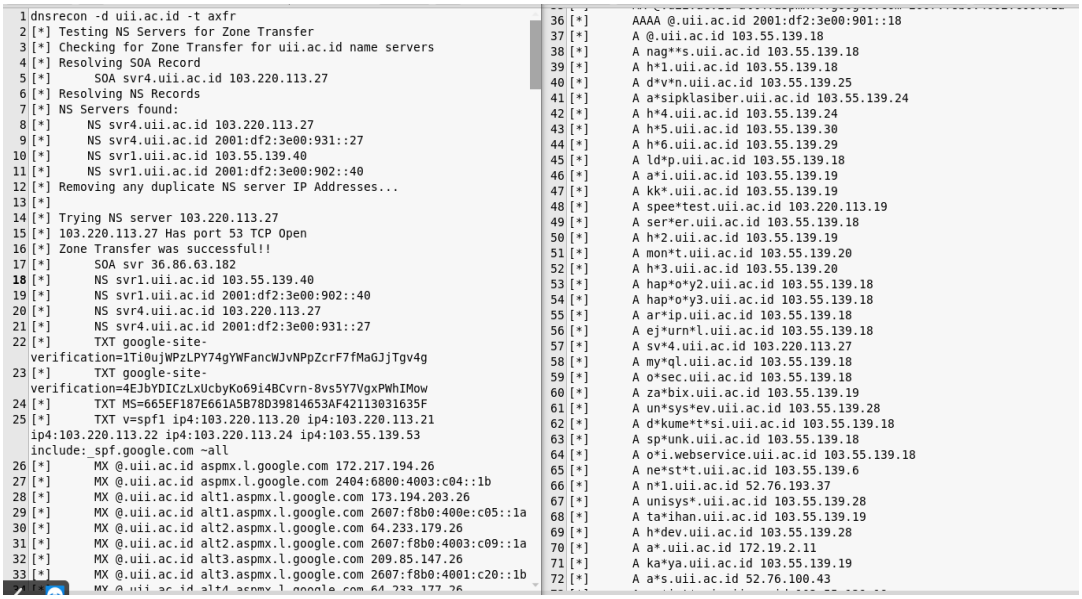
Gambar 7 Hasil pengujian DNS zone transfer

DNS zone transfer merupakan proses dimana konten berkas zona DNS disalin dari server DNS utama ke server DNS sekunder sehingga akan didapatkan semua nama domain atau sub domain yang ada pada server DNS utama. Dari hasil DNS zone transfer didapatkan beberapa URL dan IP addres yang terdapat pada svr4.uii.ac.id, svr1.uii.ac.id hasil ini menunjukan bahwa DNS server belum dikonfigurasi dengan baik karena masih mengijinkan sembarang IP address melakukan permintaan zone transfer . Lalu dengan perintah host dilakukan pengujian terhadap versi Berkeley Internet Name Domain (BIND) yang digunakan. BIND merupakan server DNS yang paling umum digunakan, hasil pengujian BIND pada Gambar 8.



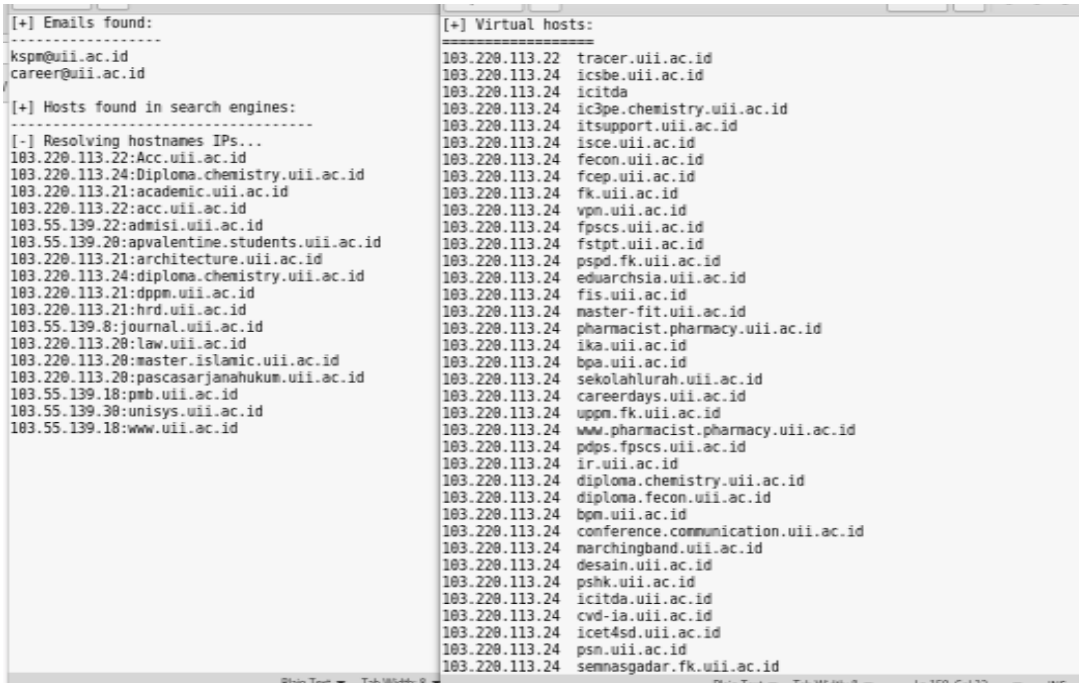
Gambar 8 hasil uji version BIND

Dari hasil pengujian BIND server tidak menjawab permintaan untuk versi BIND yang digunakan. Pengujian selanjutnya menggunakan tool dnsrecon menunjukan hasil seperti Gambar 9.



Gambar 9 Hasil pengujian dengan dnsrecon

Dengan menggunakan tool dnsrecon berhasil mendapatkan informasi dari DNS server akan tetapi *web* target yang dicari oleh penulis tidak didapatkan. Langkah berikutnya dengan cara mendatkan informasi dengan cara *crawling* di internet. Terdapat beberapa tools yag memiliki kemampuan untuk mengumpulkan informasi secara otomatis dari internet melalui search engine dengan memasukan *syntax* yang di inginkan. Gambar 10 menunjukan hasil crawling menggunakan tools theharvester dimana mendapatkan email addres,sub-domain dan juga host virtual dari sistem dan jaringan UII.



Gambar 10 Hasil *crawling*

Disini penulis berhasil menemukan *web* target yang akan dilakukan *pentest* dengan memilih secara acak memilih 6 *web* fakultas, 2 direktorat, dan 2 badan yang terdapat di UII seperti Table 2 di bawah ini.

Table 2 Daftar target

NO	FAKULTAS	Direktorat	Badan
1	www.fcep.uii.ac.id	www.dpka.uii.ac.id	www.itsupport.uii.ac.id
2	www.fis.uii.ac.id	www.humas.uii.ac.id	www.bpm.uii.ac.id
3	www.fit.uii.ac.id		
4	www.fpscs.uii.ac.id		
5	www.law.uii.ac.id		
6	www.science.uii.ac.id		

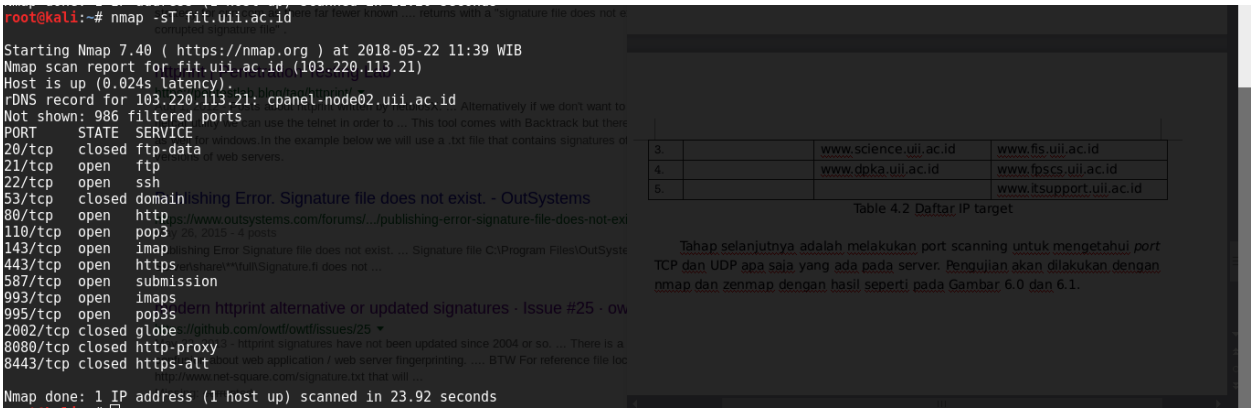
Scanning

Pada tahap ini pengujian akan lebih fokus berinteraksi langsung dengan perangkat atau sistem jaringan dari 10 *web* target yang berdomain uii.ac.id. Pada kasus ini beberapa target memiliki IP yang sama dikarenakan berupa Virtual Host maka target dikelompokan menjadi satu sesuai IP yang dimiliki seperti Table 3 untuk memudahkan dalam mencari informasi.

Table 3 Daftar IP target

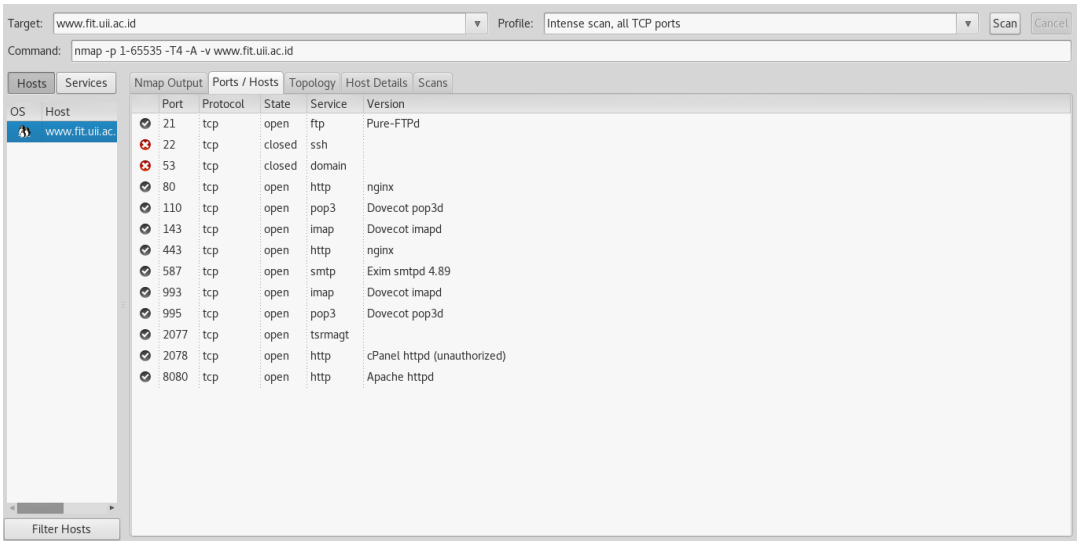
	IP		
No	103.220.113.20	103.220.113.21	103.220.113.24
1.	www.law.uii.ac.id	www.fit.uii.ac.id	www.bpm.uii.ac.id
2.		www.humas.uii.ac.id	www.fcep.uii.ac.id
3.		www.science.uii.ac.id	www.fis.uii.ac.id
4.		www.dpka.uii.ac.id	www.fpscs.uii.ac.id
5.			www.itsupport.uii.ac.id

Tahap selanjutnya adalah melakukan *port scanning* untuk mengetahui *port* TCP dan UDP apa saja yang terdapat pada server target. Pengujian dilakukan dengan beberapa tools yaitu nmap dan zenmap untuk mengetahui informasi *port scanning.* Pada kasus ini dikarenakan IP 10 *web* target berupa Virtual Host sehingga tahap *port scanning* ini dibagi hanya 3 IP sesuai table di atas. Sebagai contoh di bawah ini www.fit.uii.ac.id yang memiliki IP 103.220.113.21. Tahap ini juga dilakukan terhadap 2 IP yang lain.



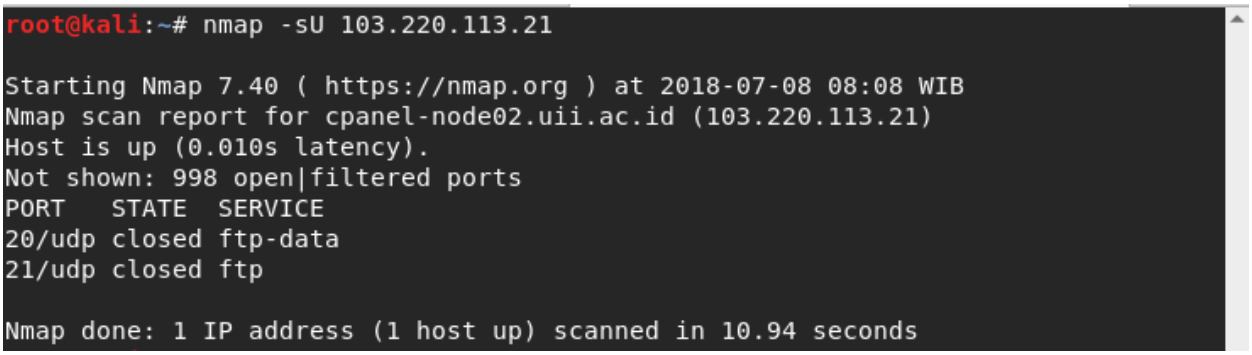
Gambar 11 Hasil *port scanning* nmap mode –sT

Hasil nmap dengan mode -sT atau *TCP connect scan* pada Gambar 11 menunjukan daftar *port* TCP yang terbuka antara lain *port* 21 untuk layanan FTP, 22 untuk layanan SSH, *port* 80 untuk layanan HTTP, *port* 110 untuk POP3, *port* 143 IMAP, *port* 443 HTTPS, *port* 587 untuk SUBMISSION, *port* 993 untuk IMAPS dan 995 untuk POP3 dari proses ini juga ditemukan bahwa *web* fit.uii.ac.id menggunakan cpanel. Selanjutnya *scanning* dilakukan menggunakan *tools* znmap.



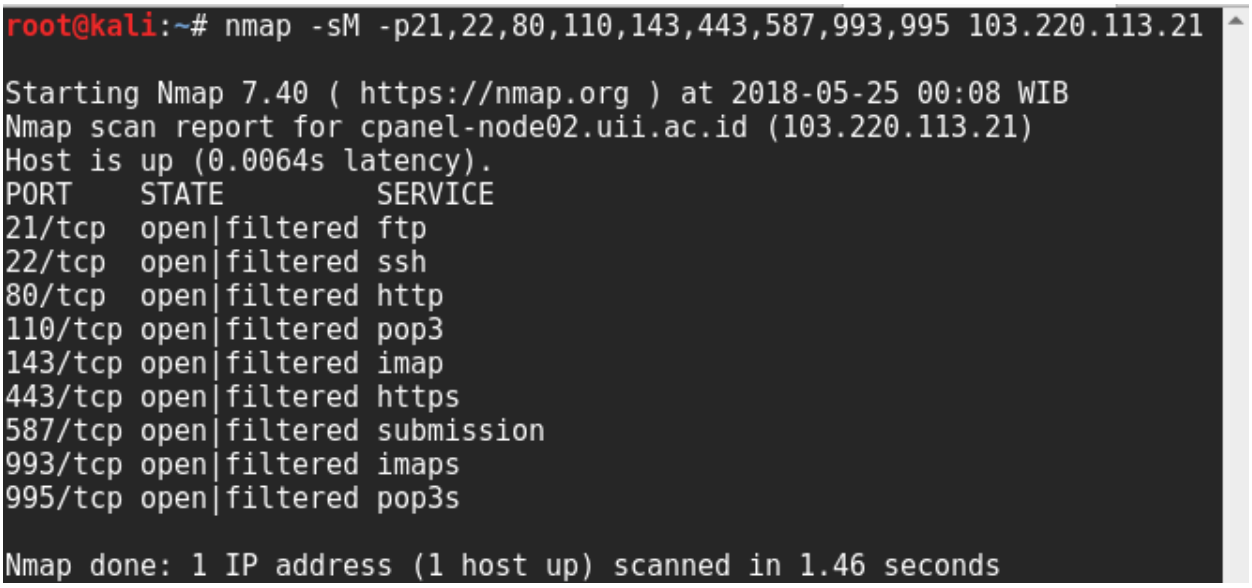
Gambar 12 Hasil *port scanning* znmap

Pada hasil *scanning* menggunakan zenmap Gambar 12 dengan *profile Intense scan, all TCP ports* menunjukan hasil yang sedikit berbeda dan jumlah *port* yang terdeteksi lebih banyak dibanding menggunakan nmap. Selanjutnya akan dilakukan *scanning* pada *port* UDP dengan menggunakan netcut dan nmap yang mana tidak ditemukan hasil *port* UDP yang terbuka seperti di tunjukan Gambar 13 ada kemungkinan paket UDP terhalangi oleh *firewall* yang terdapat dalam jaringan karena dari hasil *scanning* juga muncul notif *998 open|filtered ports.*



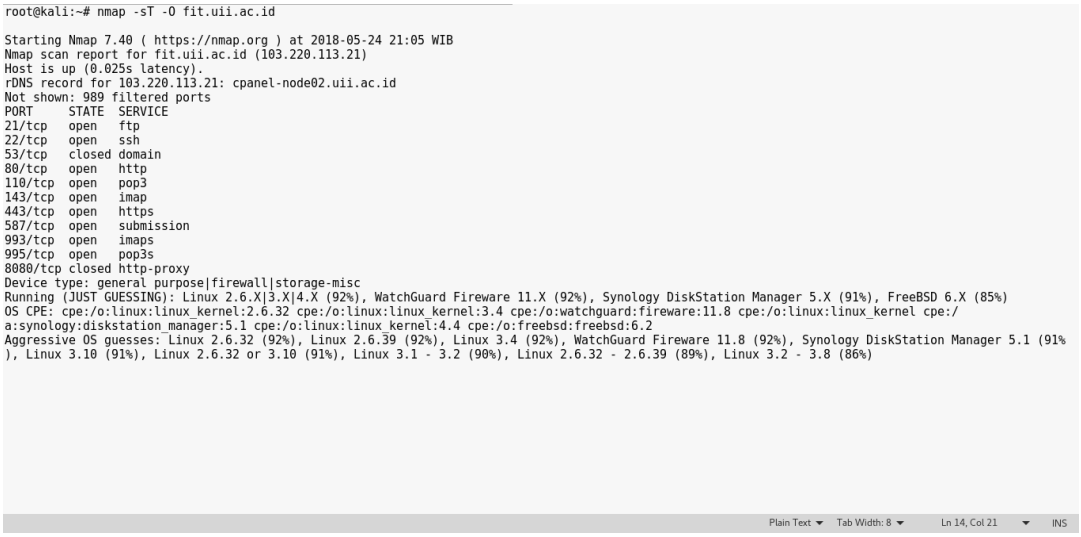
Gambar 13 *scanning* nmap mode UDP

Karena dicurigai juga terdapat *firewall* pada *port* TCP makan akan dilakukan pengujian untuk memastikan ada atau tidaknya keberadaan *firewall* dengan menggunakan *tools* nmap. Tipe *scanning* yang akan dilakukan dengan FIN/ACK *scan* atau Maimon *scan* yang mana menunjukan tahap akhir pada *three-way handshake.* Hasil *scanning* menggunakan nmap pada Gambar 14 menunjukan bawah server fit.uii.ac.id memverifikasi keberadaan *firewall* dengan menunjukan *statet open|filtered*.



Gambar 14 Hasil Maimon Scan

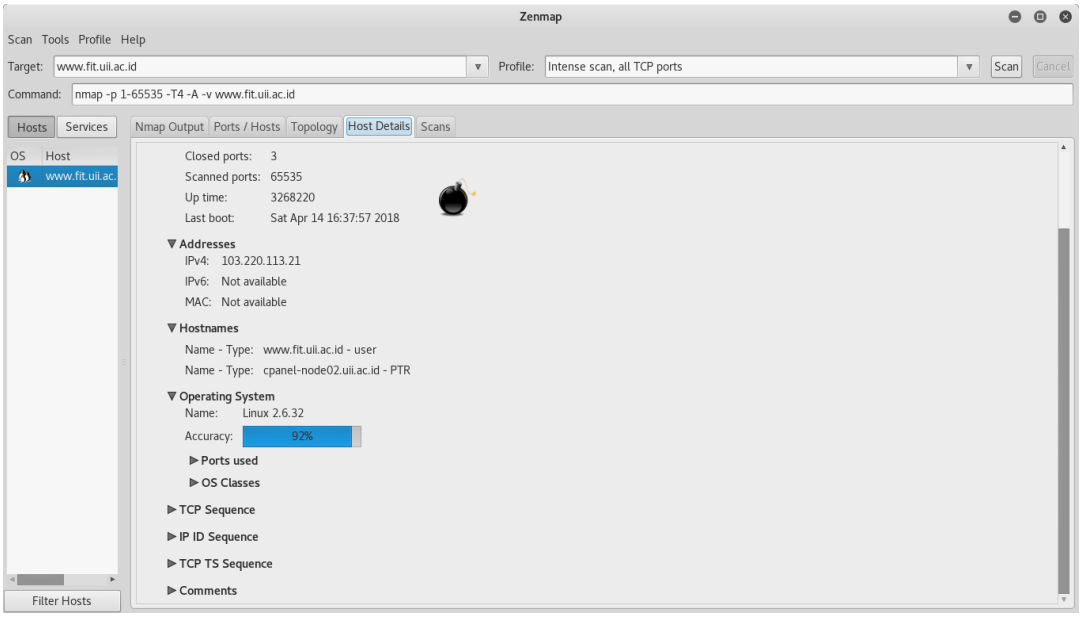
Tahap selanjutnya akan dilakukan OS *fingerprinting* untuk mengetahui jenis sistem operasi yang digunakan pada server fit.uii.ac.id. Pengujian OS *fingerprinting* akan digunakan *tools* nmap, xprobe2 dan zenmap. Hasil nmap pada Gambar 14 menunjukan bahwa sistem operasi yang digunakan adalah Linux 2.6.32 dengan tingkat akurasi sebesar 92% dan menggunakan tools xprobe2 tidak didapatkan informasi mengenai versi os target seperti ditunjukan Gambar 15 di bawah ini.



Gambar 14 OS fingerprinting dengan nmap

Gambar 15 OS fingerprinting dengan xprobe2

Selanjutnya menggunakan tools zenmap didapatkan hasil Linux 2.6.32 dengan tingkat akurasi sebesar 92% pada Gambar 16.



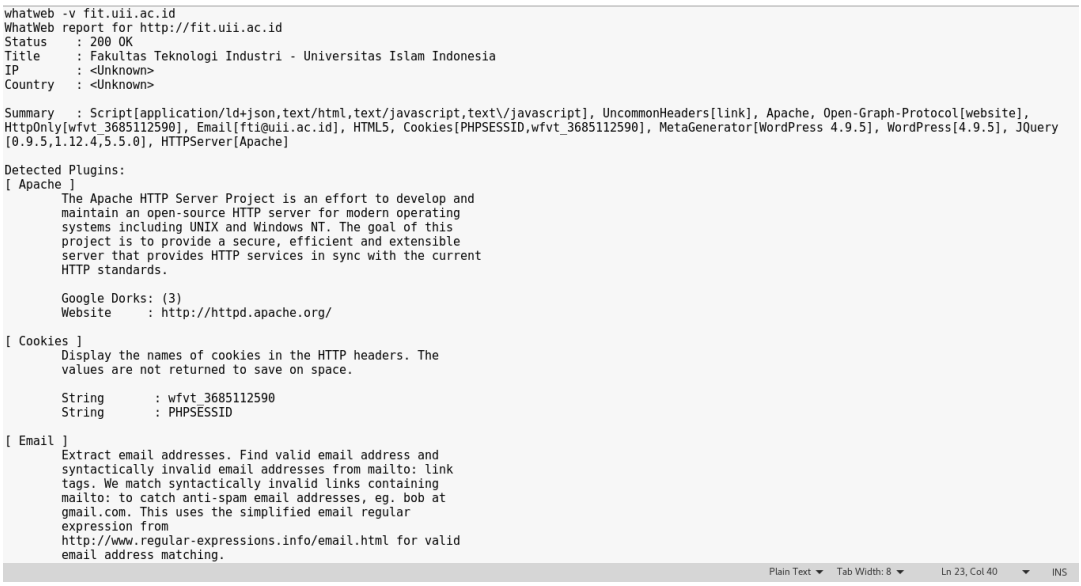
Gambar 16 OS fingerprinting dengan zenmap

Tahap selanjutnya adalah service fingerprinting untuk mengetahui layanan yang ada pada *port* yang terbuka dengan lebih jelas. *Tools* yang digunakan adalah nmap dari hasil menggunakan nmap didapatkan informasi antara lain jenis *web server* yang digunakan yaitu Apache httpd, versi SSH yaitu OpenSSH 5.3 (protocol 2.0) dan informasi lain seperti pada Gambar 17.

```
root@kali:~# nmap -sS -sV fit.uii.ac.id

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-24 22:33 WIB
Nmap scan report for fit.uii.ac.id (103.220.113.21)
Host is up (0.014s latency).
rDNS record for 103.220.113.21: cpanel-node02.uii.ac.id
Not shown: 989 filtered ports
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        Pure-FTPd
22/tcp   open   ssh        OpenSSH 5.3 (protocol 2.0)
53/tcp   closed domain
80/tcp   open   http       Apache httpd
110/tcp  open   pop3       Dovecot pop3d
143/tcp  open   imap       Dovecot imapd
443/tcp  open   ssl/ssl    Apache httpd (SSL-only mode)
587/tcp  open   smtp       Exim smtpd 4.89
993/tcp  open   ssl/imap   Dovecot imapd
995/tcp  open   ssl/pop3   Dovecot pop3d
8080/tcp closed http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.50 seconds
```

Gambar 17 Service fingerprinting dengan nmap

Kemudian untuk mengumpulkan informasi lebih banyak lagi digunakan aplikasi whatweb. Dari hasil aplikasi whatweb memberikan informasi seperti pada Gambar 18.



Gambar 18 Hasil whatweb

Hasil dari whatweb menunjukan bahwa HTTP server yang digunakan adalah Apache dan juga menunjukan bahwa *web* fit.uii.ac.id menggunakan Wordpress versi 4.9.5. Dan pada tahap ini didapatkan informasi penting yang dapat digunakan untuk tahap selanjutnya antara lain *port* dan jenis layanan pada server. Proses di atas juga diterapkan untuk pengujian pada semua *web* target yang sudah dibagi menjadi 3 alamat IP server yang ada pada Table 3 sebelumnya sehingga didapatkan hasil seperti pada Table 4, Table 5, dan Table 6 di bawah ini

Table 4 Hasil pencarian Informasi

Host IP	103.220.113.21		
Domain name	www.fit.uii.ac.id,www.humas.uii.ac.id,www.science.uii.ac.id, www.dpka.uii.ac.id		
Sistem operasi	Linux 2.6.32 (92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	Pure-FTPd
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Table 5 Hasil pencarian Informasi

Host IP	103.220.113.20		
Domain name	www.law.uii.ac.id		
Sistem operasi	Linux 2.6.32 (Kemungkinan 92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	Pure-FTPd
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Table 6 Hasil pencarian Informasi

Host IP	103.220.113.24		
Domain name	www.fcep.uii.ac.id,www.bpm.uii.ac.id,www.fis.uii.ac.id www.fpscs.uii.ac.id, www.itsupport.uii.ac.id		
Sistem operasi	Linux 2.6.32 (92%)		
Port	Layanan	Status	Versi
21	FTP	filtered	ProFTPD 1.3.5b
22	SSH	filtered	OpenSSH 5.3 (protocol 2.0)
80	HTTP	filtered	Apache httpd
110	POP3	filtered	Dovecot pop3d
143	IMAP	filtered	Dovecot imapd
443	HTTPS	filtered	Apache httpd (SSL-only mode)
587	SUBMISSION	filtered	Exim smtpd 4.89
993	IMAPS	filtered	Dovecot imapd
995	POP3S	filtered	Dovecot pop3d

Tahap selanjutnya adalah *vulnerability indentification* dimana akan dimulai mencari celah keamanan yang ada pada sistem dan server dari 10 *web* target yang berdasarkan informasi yang diperoleh sebelumnya secara manual dan dengan menggunakan *automated vulnerability scanner* yaitu WPScan dan tools otomatisasi OWASPZap yang dikembangkan penulis guna mempermudah dalam melakukan pencarian *vulnerability* target. Pada tahap sebelumnya telah diperoleh informasi bahwa server target dimungkinkan menggunakan sistem operasi Linux 2.6.32 berdasarkan informasi yang didapat sistem operasi Linux 2.6.32 memiliki beberapa kelemahan dan diantaranya memiliki nilai *Common Vulnerability Scoring System* (CVSS) sembilan atau lebih tinggi seperti yang terangkum dalam Tabel 7 yang bersumber dari salah satu database CVSS yaitu cvedetails.com (https://www. cvedetails.com)

Table 7 Celah keamanan linux 2.6.32 cvedetails.com

CVE ID	**Jenis kelemahan**	**Akses yang didapatkan**	**Auntentikasi**	**Confindentiality**	**Integrity**	**Availability**
CVE-2010-2495	DoS	Tidak ada	Tidak perlu	Complete	Complete	Complete
CVE-2009-4538	DoS	Tidak ada	Tidak perlu	Complete	Complete	Complete

Dari tabel tersebut dapat dilihat bahwa jenis kelemahaan yang terdapat pada sistem operasi Linux 2.6.32 adalah *denial of service* (DoS) yang dapat mengakibatkan terganggunya aspek-aspek keamanan informasi yaitu Confidentiality, Integrity, dan Availibility. Untuk melakukan ekseskusi terhadap kelemahaan yang terdapat pada Linux 2.6.32 juga tidak memerlukan *auntentikasi administrator* atau root cukup akses user biasa pada terminal server dan dapat mengeksekusi serangan.

Sementara itu dari informasi sebelumnya diketahui bahwa *web* target rata-rata berbasis Wordpress di sini *web* yang diuji adalah www.fpscs.uii.ac.id sehingga di sini penulis menggunakan aplikas WPScan untuk melakukan *vulnerability indentification*. Dari hasil *scanning* ditemukan kemungkinan terdapat celah kemanan seperti ditunjukan pada Table 8 di bawah ini.

Table 8 Hasil *scanning* WPScan

Jenis ancaman	**Jumlah**
Directory listing	6
Path Traversal	1
Structure & Information Disclosure	1

Dari hasil *scanning* ini juga didapatkan hasil yang dicurigai sebagai username login admin seperti Gambar 18

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+-----------+-----------+
    | Id | Login     | Name      |
    +----+-----------+-----------+
    | 1  | fpsb-uii  | fpsb uii  |
    | 2  | webmaster | webmaster |
    +----+-----------+-----------+
```

Gambar 18 Username login

Disini penulis melakukan 2kali *scanning* menggunakan *tools* WPScan pada tanggal yang berbeda dan mendapatkan hasil yang sedikit berbeda seperti di tunjukan pada Table 9.

Table 9 Perbedaan hasil WPScan

Sebelum	Sesudah
[+] WordPress version 4.8.2 (Released on 2017-09-19) identified from advanced fingerprinting, meta generator, links opml, stylesheets numbers [!] 1 vulnerability identified from the version number [!] Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset Reference: https://wpvulndb.com/vulnerabilities/8807 Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html Reference: https://core.trac.wordpress.org/ticket/25239 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295 [+] Enumerating installed plugins (only ones marked as popular) ... Plain Text Tab Width: 8 Ln 23, Col 93 INS	[+] WordPress version 4.8.6 (Released on 2018-04-03) identified from meta generator, links opml [+] Enumerating installed plugins (only ones marked as popular) ... Time: 00:06:57 <==========> (1496 / 1496) 100.00% Time: 00:06:57 [+] We found 8 plugins: [+] Name: 404-to-301 - v2.3.3 Latest version: 2.3.3 (up to date) Plain Text Tab Width: 8 Ln 22, Col 86 INS

Dari hasil yang ditunjukan Table 9 terdapat perbedaan dari versi Wordpress pada proses sebelum dan sesudah. Pada proses sebelumnya *web* www.fpscs.uii.ac.id masih menggunaka Wordpress versi 4.8.2 yang dimana dari hasil *scanning* menggunakan tools WPScan terdapat kemungkinan celah keamanan yaitu *Host Header Injection in Password Reset*. Kemudian pada proses *scanning* berikutnya Wordpress sudah di update menjadi versi 4.8.6 disini dapat disimpulkan bahwa admin cukup tanggap dalam mengelola *website* karena melakukan update secara berkala.

Selanjut dari hasil *scanning* menggunakan *tools* OWASPZap yang dikembangkan menunjukan terdapat 24 jenis kemungkinan ancaman dengan 4 kategori memiliki tingkat ancaman High, 5 kategori memiliki tingkat ancaman Medium, 15 kategori lainya memiliki tingkat ancaman Low dan 0 Informational seperti pada Gambar 19 di bawah ini dan jenis-jenis kemungkinan ancaman dari hasil *scanning* terdapat dalam Table 10.


ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	5
Low	15
Informational	0

Gambar 19 Kategori tingkat ancaman

Table 10 Hasil *scanning* tools owasp

Tingkat Ancaman	Jenis Ancaman	Jumlah
HIGH	Path Traversal	1
HIGH	Cross Site Scripting (Reflected)	1
HIGH	SQL Injection	1
HIGH	Remote OS Command Injection	1
MEDIUM	X-Frame-Options Header Not Set	3
MEDIUM	Application Error Disclosure	1
MEDIUM	Secure Pages Include Mixed Content (Including Scripts)	1
LOW	X-Content-Type-Options Header Missing	2
LOW	Cookie No HttpOnly Flag	4
LOW	Cross-Domain JavaScript Source File Inclusion	3
LOW	Password Autocomplete in Browser	2
LOW	Web Browser XSS Protection Not Enabled	1
LOW	Secure Pages Include Mixed Content	1
LOW	Incomplete or No Cache-control and Pragma HTTP Header Set	1
LOW	Cookie Without Secure Flag	1

Dan hasil seluruh *scanning* terhadap semua target dengan menggunakan langkah yang sama seperti dijelaskan sebelumnya dapat dilihat pada Tabel 11 di bawah ini

Tabel 11 hasil *scanning*

URL	Sebelum	Sesudah
www.fcep.uii.ac.id	WordPress version 4.8.1	WordPress version 4.9.5
www.fis.uii.ac.id	WordPress version 4.4.11	WordPress version 4.9.5
www.fit.uii.ac.id	WordPress version 4.4.11	WordPress version 4.9.5
www.law.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.science.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.dpka.uii.ac.id	WordPress version 4.4.11	WordPress version 4.4.15
www.itsupport.uii.ac.id	WordPress version 4.8.2	WordPress version 4.8.6
www.bpm.uii.ac.id	WordPress version 4.8.2	WordPress version 4.9.5
www.humas.uii.ac.id	-	-

Tabel 11 menunjukan hasil *scanning* menggunakan tools WPScan terhadap versi Wordpress dari semua target karena rata-rata bertipe Wordpress dari hasil tersebut menunjukan bahwa admin tanggap dalam mengelola karena telah melakukan pembaruan secara berkala terhadap versi Wordpress sebelumnya dan pada *URL* www.humas.uii.ac.id tidak mendapatkan hasil dari tools WPScan karena *web* tidak bertipe Wordpress melainkan menggunakan *JavaScript.* Selanjut pada Table 12 akan dijelaskan hasil *scanning* menggunakan aplikasi WPScan terhadap semua target akan kemungkinan terdapat celah keamanan

Table 12 Hasil *scanning* menggunakan WPScan

URL	Jenis ancaman	Jumlah	User
www.fcep.uii.ac.id	Directory listing	7	Tidak ditemukan
	Information Disclosure	1	
	SQL Injection	1	
	Path Traversal	1	
	Cross-Site Scripting (XSS)	1	
	Host Header Injection in Password Reset	1	
www.fis.uii.ac.id	Directory listing	10	Ditemuka
	Cross-Site Scripting (XSS)	1	
	Host Header Injection in Password Reset	1	
www.fit.uii.ac.id	Directory listing	7	Tidak Ditemukan
	Remote Path Traversal File Access	1	
	Style Editing CSRF	1	
	Authenticated Stored XSS & SQL Injection	1	
	Information Disclosure	1	
	Host Header Injection in Password Reset	1	
www.law.uii.ac.id	Directory listing	10	Tidak Ditemukan
	Host Header Injection in Password Reset	1	
	Style Editing CSRF	3	
	Remote Path Traversal File Access	1	
	Cross-Site Scripting (XSS)	8	

URL	Jenis ancaman	Jumlah	User
	SQL Injection	4	
	Multiple vulnerabilities in login CAPTCHA	1	
	information Disclosure	1	
	File Upload Remote Code Execution	1	
www.science.uii.ac.id	Cross-Site Scripting (XSS)	1	
	Directory listing	2	Ditemuka
	information Disclosure	1	
	Host Header Injection in Password Reset	1	
www.dpka.uii.ac.id	Cross-Site Scripting (XSS)	2	
	Host Header Injection in Password Reset	1	Ditemuka
	Revolution Local File Disclosure	1	
	Revolution Shell Upload	1	
	Directory listing	4	
www.itsupport.uii.ac.id	Directory listing	11	Ditemukan
	Host Header Injection in Password Reset	1	
	Cross-Site Scripting (XSS)	1	
	Authenticated PHP Object Injection	1	
www.bpm.uii.ac.id	Cross-Site Scripting (XSS)	3	Ditemukan
	Directory listing	6	
	Host Header Injection in Password Reset	1	
	CSRF	3	
	Authenticated Multisite Remote Code Execution	1	
	Information Disclosure	1	
	Missing Settings Authorization	1	
	Revolution Local File Disclosure	1	
	Revolution Shell Upload	1	
	Open Redirect	1	
www.humas.uii.ac.id	-	-	-

Dari hasil *scanning* menggunakan WPScan pada Table 12 hanya www.humas.uii.ac.id yang tidak terdapat hasil *scannig* dikarenakan *web* www.humas.uii.ac.id tidak bertipe Wordpress seperti yang sudah dijelaskan sebelumnya. Selanjutnya hasil dari *scanning* menggunaka tools otomatisasi OWASPZap yang dikembangkan terdapat pada Table 13 di bawah ini.

Table 13 Hasil *scanning* otomatisasi OWASPZap

URL	Tingkat Ancaman	Jenis Ancaman	jumlah
www.fcep.uii.ac.id	HIGH	Path Traversal	1
	MEDIUM	X-Frame-Options Header Not Set	2
	MEDIUM	Application Error Disclosure	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	2
	LOW	Cross-Domain JavaScript Source File Inclusion	1
www.fis.uii.ac.id	MEDIUM	X-Frame-Options Header Not Set	6
	MEDIUM	Application Error Disclosure	1
	LOW	Web Browser XSS Protection Not Enabled	4
	LOW	Cookie No HttpOnly Flag	4
	LOW	X-Content-Type-Options Header Missing	10
	LOW	Content-Type Header Missing	2
	LOW	Cross-Domain JavaScript Source File Inclusion	4
	LOW	Private IP Disclosure	1
www.fit.uii.ac.id	HIGH	Cross Site Scripting (Reflected)	1
	HIGH	Remote OS Command Injection	1
	HIGH	Path Traversal	1
	HIGH	SQL Injection	1
	MEDIUM	X-Frame-Options Header Not Set	2

URL	Tingkat Ancaman	Jenis Ancaman	jumlah
	MEDIUM	Directory Browsing	1
	MEDIUM	Application Error Disclosure	2
	MEDIUM	Format String Error	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	2
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie Without Secure Flag	1
	LOW	Incomplete or No Cache-control and Pragma HTTP Header Set	1
	LOW	Secure Pages Include Mixed Content	1
www.law.uii.ac.id	HIGH	Remote OS Command Injection	1
	HIGH	SQL Injection	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	X-Content-Type-Options Header Missing	1
	LOW	Cookie No HttpOnly Flag	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Web Browser XSS Protection Not Enabled	1
	LOW	Password Autocomplete in Browser	1
www.science.uii.ac.id	HIGH	Path Traversal	1
	HIGH	Remote OS Command Injection	1
	MEDIUM	X-Frame-Options Header Not Set	1

URL	Tingkat Ancaman	Jenis Ancaman	jumlah
	MEDIUM	Application Error Disclosure	1
	MEDIUM	Format String Error	1
	LOW	Cookie No HttpOnly Flag	1
	LOW	Private IP Disclosure	1
	LOW	Password Autocomplete in Browser	1
www.dpka.uii.ac.id	HIGH	SQL Injection	1
	HIGH	Remote OS Command Injection	1
	HIGH	Path Traversal	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
www.itsupport.uii.ac.id	HIGH	Remote OS Command Injection	
	HIGH	Remote File Inclusion	
	HIGH	Path Traversal	
	HIGH	SQL Injection	
	MEDIUM	Application Error Disclosure	1
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie No HttpOnly Flag	2
	LOW	Password Autocomplete in Browser	1
	LOW	Private IP Disclosure	1
	LOW	X-Content-Type-Options Header Missing	1
www.bpm.uii.ac.id	HIGH	Path Traversal	1
	HIGH	Remote OS Command Injection	1

URL	Tingkat Ancaman	Jenis Ancaman	jumlah
	MEDIUM	X-Frame-Options Header Not Set	1
	MEDIUM	Directory Browsing	1
	MEDIUM	Format String Error	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Password Autocomplete in Browser	1
	LOW	Cookie No HttpOnly Flag	1
www.humas.uii.ac.id	HIGH	SQL Injection	1
	MEDIUM	Directory Browsing	1
	MEDIUM	X-Frame-Options Header Not Set	1
	LOW	Cross-Domain JavaScript Source File Inclusion	1
	LOW	Cookie No HttpOnly Flag	1

Selanjut penulis mencoba melakukan *scanning* menggunakan Whatwaf untuk mencaritau *firewall* apa saja yang terdapat pada *web* target karena dicurigai *web* memiliki *firewall* dari proses yang telah dilakukan sebelumnya. Dari hasil *scanning* terdapat beberapa *firewall* yang terdeteksi pada *web* target yang antara lain dapat dilihat pada Table 14 di bawah ini.

Table 14 Daftar nama *firewall* yang terdeteksi aplikasi WhatWaf

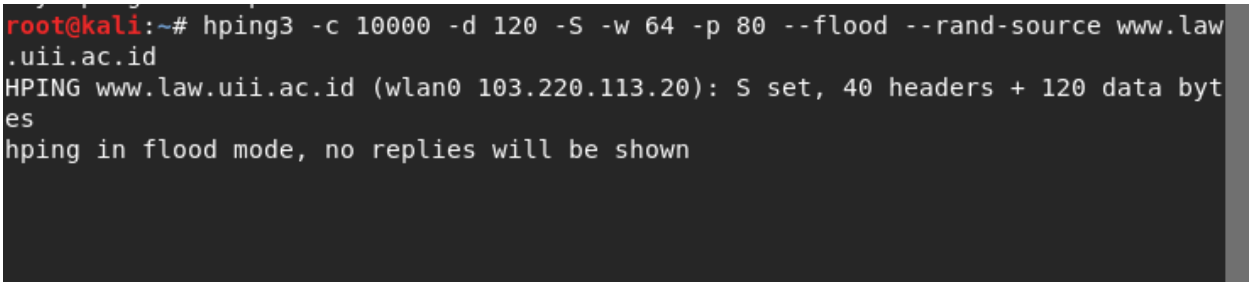
URL	Firewall
www.fis.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fit.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fpscs.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.law.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.bpm.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.science.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.fcep.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.dpka.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.humas.uii.ac.id	SafeDog WAF (SafeDog)
	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection
www.itsupport.uii.ac.id	Palo Alto Firewall (Palo Alto Networks)
	Apache generic website protection

Uji kemungkinan celah

Pada tahap ini dilakukan pengujian terhadapa kemungkinan celah kemanan yang telah ditemukan pada tahap sebelumnya.

Denial of Service (DoS)

Menurut www.cvedetails.com bahwa sistem operasi Linux 2.6.32 memiliki kemungkinan celah keamanan DoS sehingga perlu dilakukan pengujian serangan DoS. Disini penguji menggunakan tools hping3 dan slowhttptest dalam melakukan serangan DoS terhadap *web* target serangan ini bertipe *three way handshake* dimana penyerang membanjiri *web server* dengan request berupa paket *SYN* . *SYN* paket adalah paket dari client yang mengawali terbentuknya koneksi *Tcp/Ip*, setelah itu server akan membalas dengan *SYN-ACK*, dan dilengkapi dengan paket *SYN-ACK-ACK* dari client.



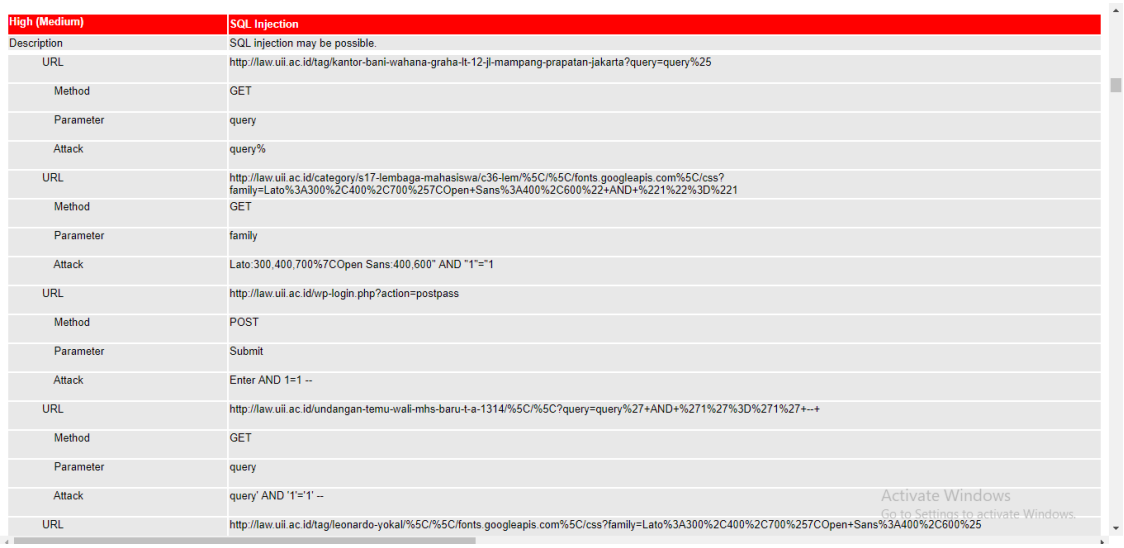
Gambar 20 Serangan DoS dengan hping3

Gambar 21 Serangan DoS menggunakan Slowhttptest

Pada Gambar 20 dan Gambar 21 serangan ditunjukan kepada *web* law.uii.ac.id namun dari serangan DoS *website* law.uii.ac.id tidak terpengarahui sama sekali terhadap serangan besar kemungkinan *web* law.uii.ac.id sudah menggunakan load balancing. Percobaan serangan DoS juga dilakukan terhadap semua *web* target akan tetapi hasilnya sama seperti *web* law.uii.ac.id *web* target lainya sama sekali tidak ada masalah.

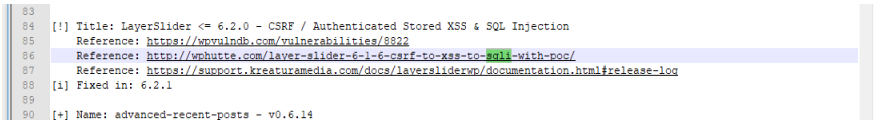
SQL Injection

Pada proses sebelumnya terdeteksi bahwa beberapa *web* target memiliki kemungkinan celah keaman SQL Injection seperti di tunjukan pada Gambar 22 dan Gambar 23.



High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://law.uii.ac.id/tag/kantor-bani-wahana-graha-lt-12-jl-mampang-prapatan-jakarta?query=query%25
Method	GET
Parameter	query
Attack	query%
URL	http://law.uii.ac.id/category/s17-lembaga-mahasiswa/c36-lem/%5C/%5C/fonts.googleapis.com%5C/css?family=Lato%3A300%2C400%2C700%257COpen+Sans%3A400%2C600%22+AND+%221%22%3D%221
Method	GET
Parameter	family
Attack	Lato:300,400,700%7COpen Sans:400,600" AND "1"="1
URL	http://law.uii.ac.id/wp-login.php?action=postpass
Method	POST
Parameter	Submit
Attack	Enter AND 1=1 --
URL	http://law.uii.ac.id/undangan-temu-wali-mhs-baru-t-a-1314/%5C/%5C?query=query%27+AND+%271%27%3D%271%27+--+
Method	GET
Parameter	query
Attack	query' AND '1'='1' --
URL	http://law.uii.ac.id/tag/leonardo-yokal/%5C/%5C/fonts.googleapis.com%5C/css?family=Lato%3A300%2C400%2C700%257COpen+Sans%3A400%2C600%25

Gambar 22 Kemungkinan terdapat celah SQL Injection menurut aplikasi otomatisasi OWASPZap



```
83
84  [!] Title: LayerSlider <= 6.2.0 - CSRF / Authenticated Stored XSS & SQL Injection
85      Reference: https://wpvulndb.com/vulnerabilities/8822
86      Reference: http://wphutte.com/layer-slider-6-1-6-csrf-to-xss-to-sqli-with-poc/
87      Reference: https://support.kreaturamedia.com/docs/layersliderwp/documentation.html#release-log
88  [i] Fixed in: 6.2.1
89
90  [+] Name: advanced-recent-posts - v0.6.14
```

Gambar 23 Hasil *scanning* menggunakan WPScan kemungkinan terdapat celah SQL Injection

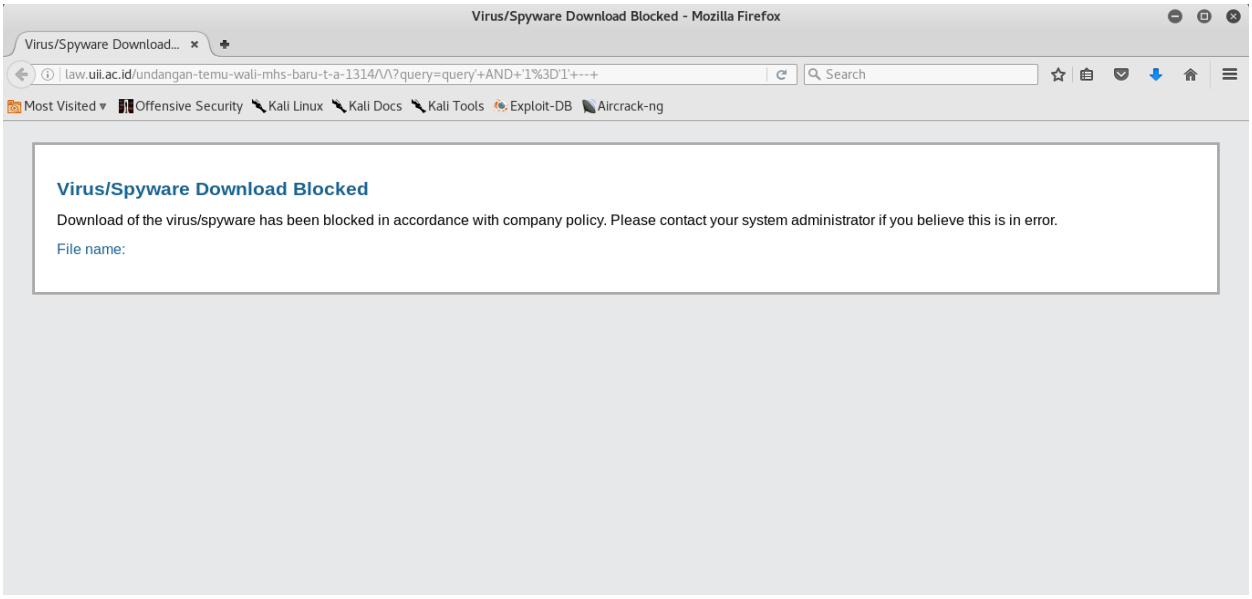
Dari proses *scanning* tahap sebelumnya menggunakan tools otomatisasi OWASPZap dan WPScan ditemukan kemungkinan celah keamana serangan SQL Injection pada *web* www.law.uii.ac.id

tidak hanya terdapat dalam *web* law.uii.ac.id saja kemungkinan ini juga teridentifikasi pada beberapa *web* target diantaranya dapat dilihat pada Table 15 di bawah ini.

Table 15 Kemungkinan *web* terdapat celah SQLI

www.fpscs.uii.ac.id
www.humas.uii.ac.id
www.itsupport.uii.ac.id
www.dpka.uii.ac.id
www.fit.uii.ac.id
www.fcep.uii.ac.id

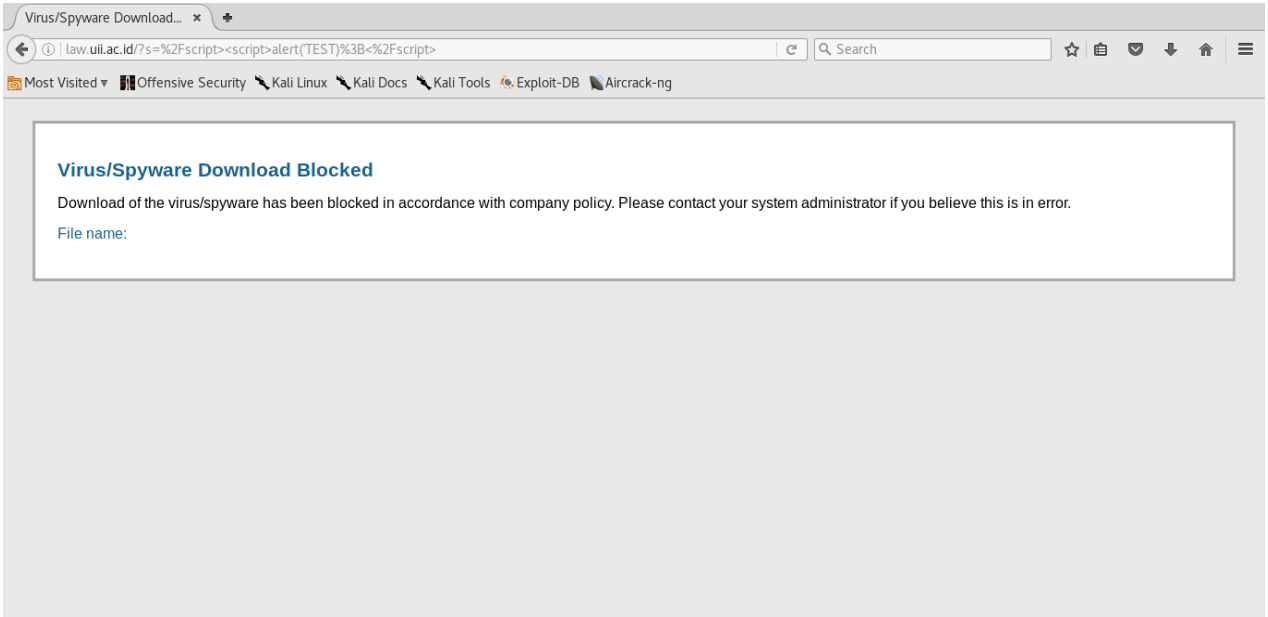
Dari kemungkinan ini dilakukan pembuktian dengan pengujian secara manual menggunakan browser. Selanjutnya pengujian dilakukan secara manual dengan memasukan query tertentu dalam URL target dan hasilnya seperti ditunjukan pada Gambar 25 dimana query yang dimasukan langsung terdeteksi oleh *firewall* yang dimiliki dan langsung dicegah oleh *firewall.*



Gambar 25 Serangan SQL Injection secara manual

Cross-Site Scripting (XSS)

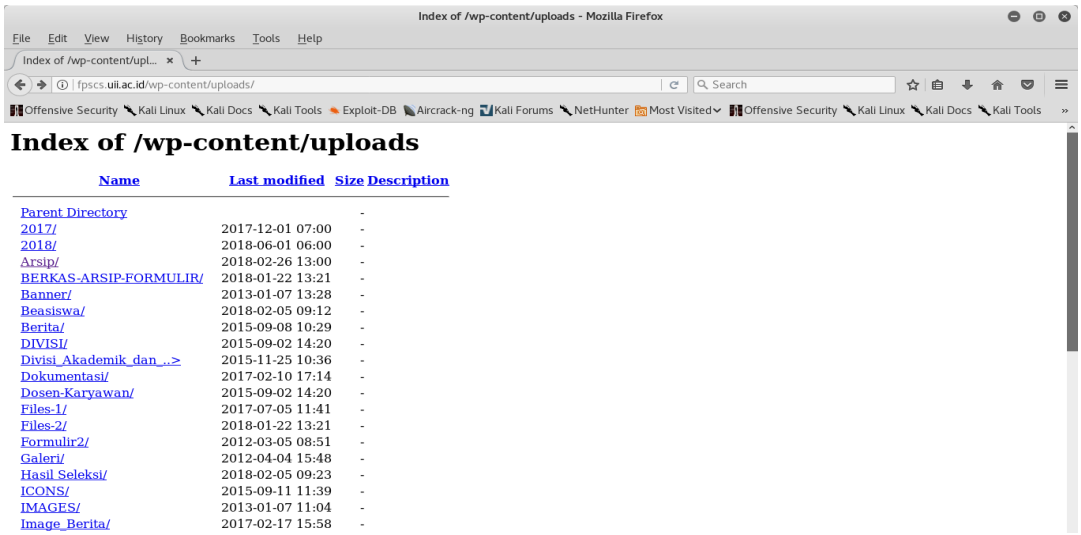
XSS adalah salah satu jenis serangan injeksi code *(code injection attack)*. XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau *client script code* lainnya ke suatu situs. Kemungkinan celah keamanan ini juga ditemukan hampir pada semua *web* target sehingga perlu dilakukan pengujian. Disini penguji melakukan serangan XSS secara manual dengan browser dan memasukan *code injeksi* ke dalam *web* target. Akan tetapi serangan yang dilakukan penguji terdeteksi oleh *firewall* sehingga langsung dicegah oleh *firewall* seperti yang ditunjukan Gambar 26.



Gambar 26 Hasil serangan XSS

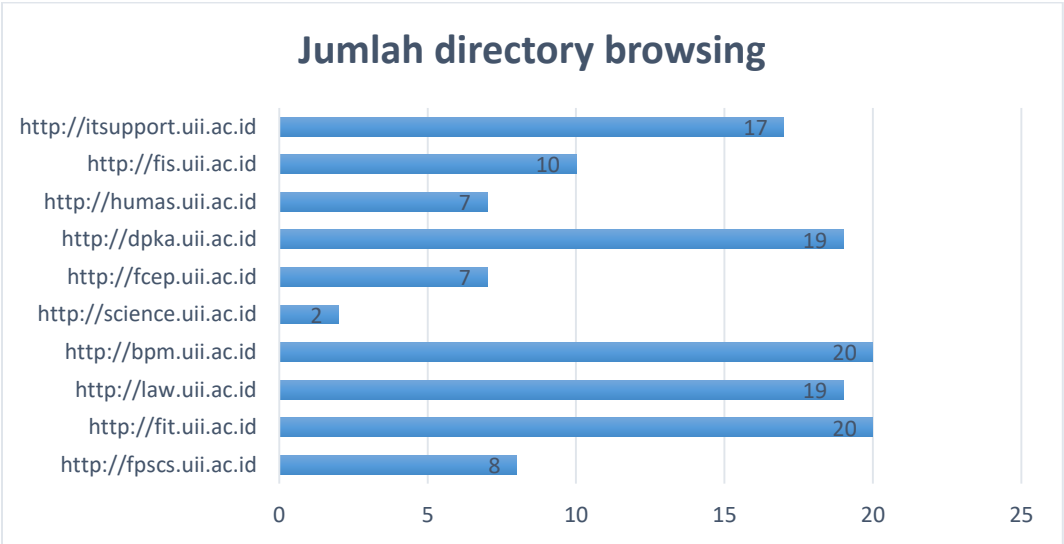
Directory Browsing

Directory Browsing adalah celah keamanan dimana orang yang tidak memiliki hak akses terhadap suatu *website* dapat mengakses halaman yang berupa informasi informasi sensitif pada suatu *website* tertentu. Pada kasus ini kemungkinan celah keamanan ini terdeteksi pada proses *scanning* dan hampir terdeteksi pada seluruh *web* target sehingga perlu dilakukan pengujiaan lagi dengan mencoba melakukan akses terhadap Directory yang ditemukan pada proses sebelumnya seperti Gambar 27 di bawah ini



Gambar 27 Directory browsing pada *URL* www.fpscs.uii.ac.id

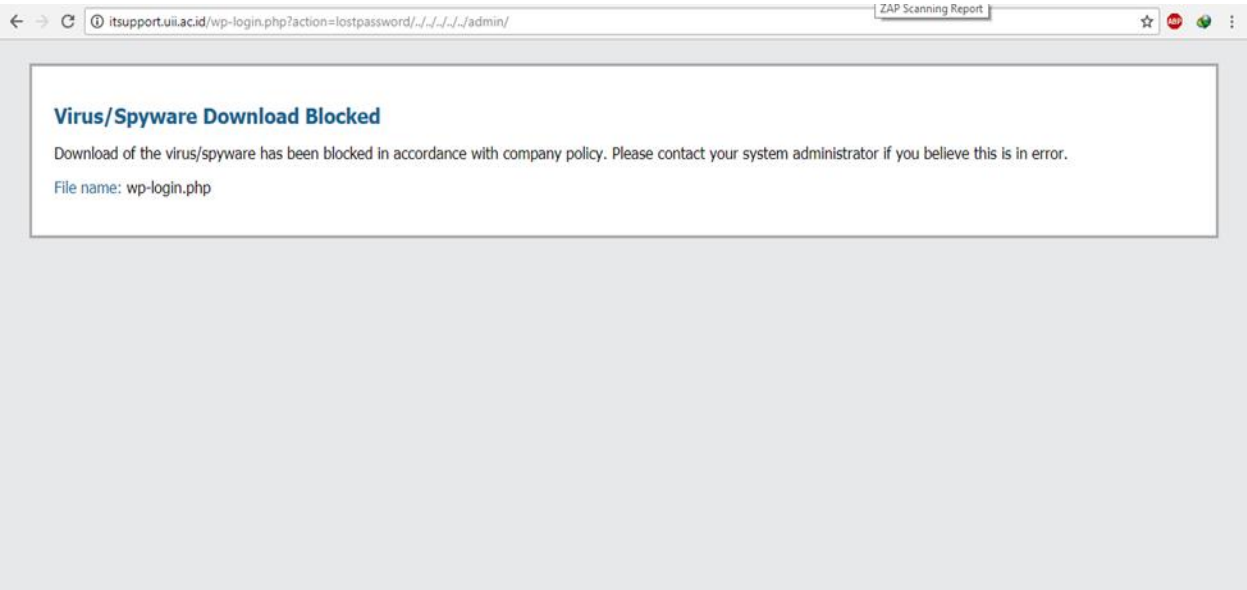
Dari Gambar 27 didapatkan informasi mengenai file apa saja yang terdapat dalam *web* www.fpscs.uii.ac.id dan informasi tanggal terakhir admin melakukan perubahaan pada file tersebut. Dari proses pengujian ini didapatkan hasil seperti pada Gambar 28 grafik yang menunjukan jumlah *Directory Browsing* yang dapat diakses pada setiap *web* target.



Gambar 28 Grafik *web* yang memiliki celah Directory Browsing

Path Traversal

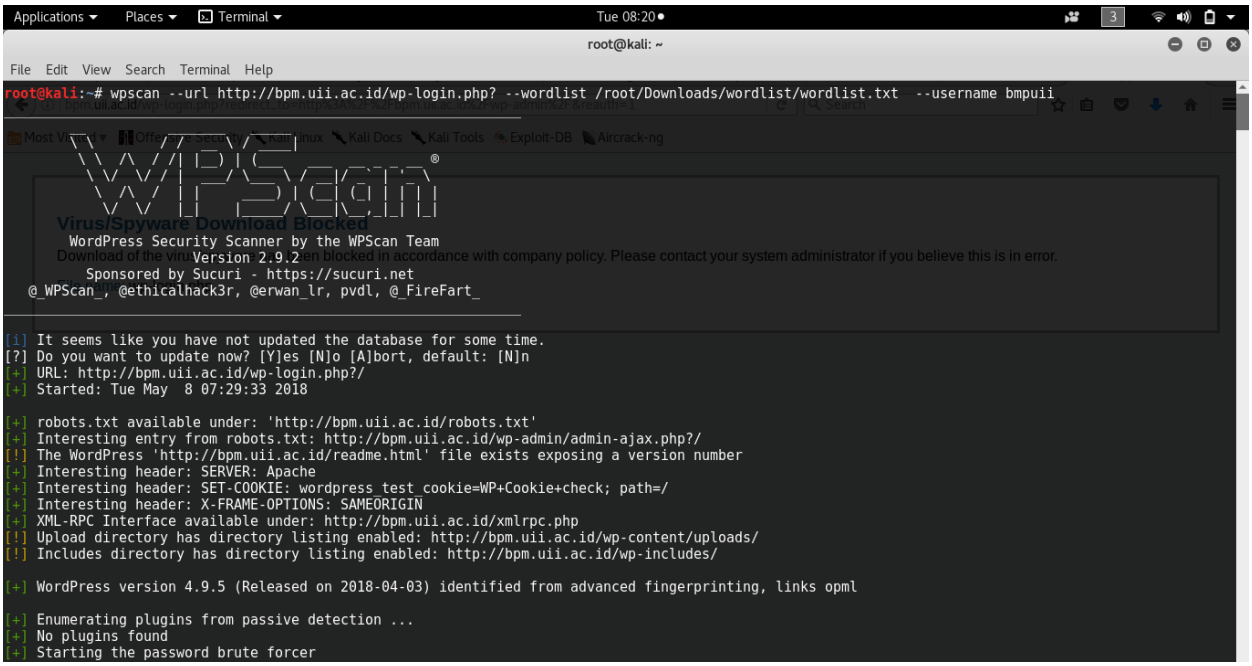
Path traversal adalah ekspolitasi pada *HTTP* yang dapat memberikan akses tidak sah kepada orang yang tidak memiliki hak akses tersebut. Pada kasus ini juga ditemukan kemungkinan celah keamana Path traversal sehingga perlu dilakukan pengujian. Disini penguji menggunakan browser dalam melakukan serangan Path Traversal dengan memasukan query pada HTTP target akan tetapi serangan berhasil terdetekti oleh *firewall* dan langsung dicegah seperti ditunjukan Gambar 29.



Gambar 29 Injeksi serangan Path Traversal

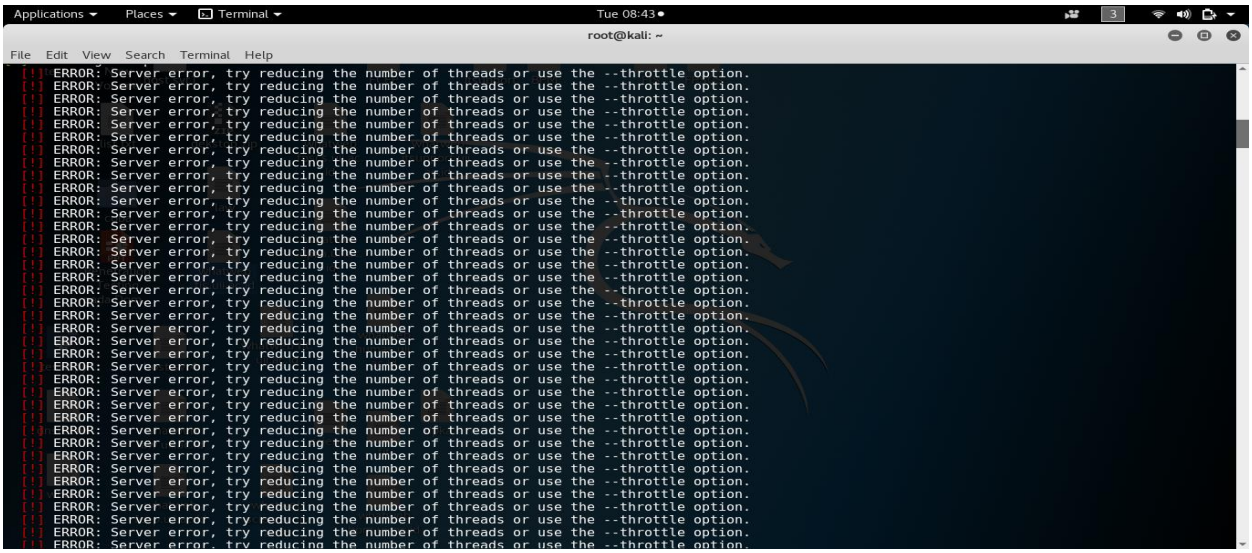
Sensitive Data Exposure

Pada proses *scanning* menggunakan tools WPScan ditemukan beberapa userlogin pada *web* target sehingga perlu dilakukan pengujian. Disini penulis melakukan pengujian terhadap kemungkinan user login yang ditemukan pada tahap sebelumnya menggunakan aplikasi WPScan dengan metode *brute force* yang berjenis *dictionary attack* dengan menggunakan user login yang sudah ditemukan sebelumnya dan untuk mencari password menggunakan *dictionary password* yang terdapat pada Kali linux yang memiliki jumlah kata sekitar 13 juta. Serangan dilakukan terhadap halaman form login *web* target disini penulis melakukan pengujian terhadap www.bpm.uii.ac.id seperti pada Gambar 30 di bawah ini.



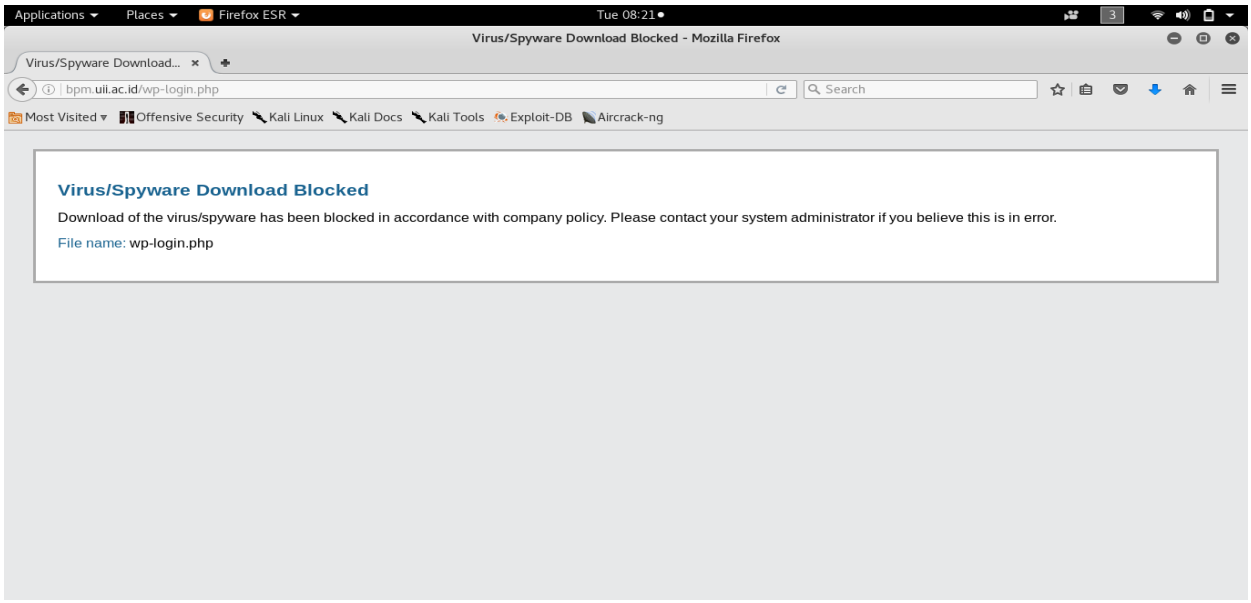
Gambar 30 Serangan *brute force* dengan WPScan

Hasil serangan *brute force* menggunakan aplikasi WPScan dinyatakan tidak berhasil dikarenakan langsung terjadi notification *server eror* seperti pada Gambar 31 yang kemungkinan besar serangan yang dilakukan langsung dicegah oleh *firewall* yang di miliki oleh *web* target.



Gambar 31 Hasil serangan *brute force* dengan WPScan

Kemungkinan serangan dicegah oleh *firewall* yang dimiliki oleh *web* target dikuatkan dengan penulis yang mencoba melakukan akses menggunakan browser ke halaman login *web* target dan terdapat peringatan seperti yang ditunjukan pada Gambar 32 di bawah ini.



Gambar 32 Akses halaman login *web* target

Selama proses *brute force* dijalankan semua akses ke halaman login *web* taget yang menggunakan *gateway* yang sama tidak dapat dilakukan dan akan otomatis muncul peringatan seperti Gambar 32 di atas. Setelah proses *brute force* dihentikan dan menunggu kurang lebih 5menit halaman login dapat diakses secara normal kembali. Proses ini juga dilakukan terhadap semua kemungkinan userlogin yang ditemukan pada tahap sebelumnya.

Rekomendasi

Setelah melakukan proses *penetration testing* terhadap 10 *web* yang berdomain uii.ac.id dan melakukan analisa lebih dalam terhadap hasil uji penulis memiliki beberapa rekomendasi Antara lain:

1. Melakukan konfigurasi kembali pada DNS server agar mengijinkan IP addres yang sudah ditentukan saja yang dapat melaukan permintaan zone transfer
2. Melakukan disable directori browsing melalui CPanel atau dapat melakukan pemblokiran menggunakan file .htacces
3. Melakuka update secara berkala terhadap sistem yang digunakan untuk mencegah celah keamanan baru yang muncul seperti pada *plugin* yang digunakan
4. Perlu dilakukan encryption terhadap data yang penting untuk mengurangi resiko terjadinya kebocoran informasi yang sensitif
5. Melakukan pengaturan agar *web* yang bertipe Wordpress tidak dapat di *scan* menggunakan aplikasi WPScan dengan cara melakukan pengaturan pada file.htaces yaitu mengganti nama folder bawaan Wordpress dengan nama lainya

Law.uii.ac.id	
Hasil pertama	Hasil kedua
root@kali:~# wpscan --url www.law.uii.ac.id --enumerate p,u,t _____ _____ __ _____ _____ \ \ / / __ \ / ____| \ \ /\ / /| |__) | (___ ___ __ _ _ __ ® \ \/ \/ / | ___/ ___ \ / __|/ _` | '_ \ \ /\ / | | ____) | (__| (_| | | | \/ \/ |_| |_____/ ___|__,_|_| |_| WordPress Security Scanner by the WPScan Team Version 2.9.2 Sponsored by Sucuri - https://sucuri.net @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_ _____ _____ [i] The remote host tried to redirect to: http://law.uii.ac.id/ [?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y [+] URL: http://law.uii.ac.id/ [+] Started: Thu Oct 12 06:17:58 2017 [+] robots.txt available under: 'http://law.uii.ac.id/robots.txt' [+] Interesting entry from robots.txt: http://law.uii.ac.id/wp-admin/admin-ajax.php [!] The WordPress 'http://law.uii.ac.id/readme.html' file exists exposing a version number [+] Interesting header: LINK: <http://law.uii.ac.id/wp-json/>; rel="https://api.w.org/", <http://law.uii.ac.id/>; rel=shortlink [+] Interesting header: SERVER: nginx [+] Interesting header: SET-COOKIE: wfvt_2115448279=59dea6b17707e; expires=Wed, 11-Oct-2017 23:48:09 GMT; Max-Age=1800; path=/; httponly [+] Interesting header: X-CONTENT-TYPE-OPTIONS: nosniff	root@kali:~# wpscan --url www.law.uii.ac.id --enumerate p,u,t _____ _____ __ _____ _____ \ \ / / __ \ / ____| \ \ /\ / /| |__) | (___ ___ __ _ _ __ ® \ \/ \/ / | ___/ ___ \ / __|/ _` | '_ \ \ /\ / | | ____) | (__| (_| | | | \/ \/ |_| |_____/ ___|__,_|_| |_| WordPress Security Scanner by the WPScan Team Version 2.9.2 Sponsored by Sucuri - https://sucuri.net @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_ _____ _____ [i] The remote host tried to redirect to: http://law.uii.ac.id/ [?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y [+] URL: http://law.uii.ac.id/ [+] Started: Wed Apr 18 06:11:55 2018 [+] robots.txt available under: 'http://law.uii.ac.id/robots.txt' [+] Interesting entry from robots.txt: http://law.uii.ac.id/wp-admin/admin-ajax.php [!] The WordPress 'http://law.uii.ac.id/readme.html' file exists exposing a version number [+] Interesting header: LINK: <http://law.uii.ac.id/wp-json/>; rel="https://api.w.org/", <http://law.uii.ac.id/>; rel=shortlink [+] Interesting header: SERVER: Apache [+] Interesting header: SET-COOKIE: wfvt_2115448279=5ad67f3c89a2a; expires=Tue, 17-Apr-2018 23:41:56 GMT; Max-Age=1800; path=/; httponly [+] Interesting header: X-TEC-API-ORIGIN: http://law.uii.ac.id

```
[+] Interesting header: X-NGINX-CACHE-STATUS: MISS
[+] Interesting header: X-SERVER-POWERED-BY: BSI UII
[+] Interesting header: X-XSS-PROTECTION: 1; mode=block
[+] XML-RPC Interface available under: http://law.uii.ac.id/xmlrpc.php
[!] Upload directory has directory listing enabled: http://law.uii.ac.id/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://law.uii.ac.id/wp-includes/

[+] WordPress version 4.8.2 (Released on 2017-09-19) identified from advanced fingerprinting, meta generator, links opml, stylesheets numbers
[!] 1 vulnerability identified from the version number

[!] Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset
   Reference: https://wpvulndb.com/vulnerabilities/8807
   Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
   Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
   Reference: https://core.trac.wordpress.org/ticket/25239
   Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

[+] WordPress theme in use: uoc-theme - v1.1

[+] Name: uoc-theme - v1.1
 |  Location: http://law.uii.ac.id/wp-content/themes/uoc-theme/
 |  Readme: http://law.uii.ac.id/wp-content/themes/uoc-theme/readme.txt
 |  Style URL: http://law.uii.ac.id/wp-content/themes/uoc-theme/style.css
 |  Theme Name: Uoc Theme
 |  Theme URI: http://themeforest.net/user/chimpstudio
```

```
[+] Interesting header: X-TEC-API-ROOT: http://law.uii.ac.id/wp-json/tribe/events/v1/
[+] Interesting header: X-TEC-API-VERSION: v1
[+] XML-RPC Interface available under: http://law.uii.ac.id/xmlrpc.php
[!] Upload directory has directory listing enabled: http://law.uii.ac.id/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://law.uii.ac.id/wp-includes/

[+] WordPress version 4.9.5 (Released on 2018-04-03) identified from advanced fingerprinting, meta generator, links opml, stylesheets numbers

[+] Enumerating installed plugins (only ones marked as popular) ...

  Time: 00:23:42 <======================> (1496 / 1496) 100.00% Time: 00:23:42

[+] We found 18 plugins:

[+] Name: 404-to-301 - v2.3.3
 |  Latest version: 2.3.3 (up to date)
 |  Location: http://law.uii.ac.id/wp-content/plugins/404-to-301/
 |  Readme: http://law.uii.ac.id/wp-content/plugins/404-to-301/readme.txt

[+] Name: LayerSlider
 |  Location: http://law.uii.ac.id/wp-content/plugins/LayerSlider/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: LayerSlider 4.6.1 - Style Editing CSRF
   Reference: https://wpvulndb.com/vulnerabilities/7152
   Reference: http://packetstormsecurity.com/files/125637/
[i] Fixed in: 5.2.0

[!] Title: LayerSlider 4.6.1 - Remote Path Traversal File Access
   Reference: https://wpvulndb.com/vulnerabilities/7153
```

| Description: UOCE (University of College Education) is elegant, customizable, easy, and clear WordPress theme....
| Author: Chimpstudio
| Author URI: http://themeforest.net/user/chimpstudio

[+] Enumerating installed plugins (only ones marked as popular) ...

Time: 00:37:26 <=======================> (1500 / 1500) 100.00% Time: 00:37:26

[+] We found 22 plugins:

[+] Name: 404-to-301 - v2.3.3
| Latest version: 2.3.3 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/404-to-301/
| Readme: http://law.uii.ac.id/wp-content/plugins/404-to-301/readme.txt

[+] Name: LayerSlider
| Location: http://law.uii.ac.id/wp-content/plugins/LayerSlider/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: LayerSlider 4.6.1 - Style Editing CSRF
Reference: https://wpvulndb.com/vulnerabilities/7152
Reference: http://packetstormsecurity.com/files/125637/
[i] Fixed in: 5.2.0

[!] Title: LayerSlider 4.6.1 - Remote Path Traversal File Access
Reference: https://wpvulndb.com/vulnerabilities/7153
Reference: http://packetstormsecurity.com/files/125637/
Reference: https://secunia.com/advisories/57309/
[i] Fixed in: 5.2.0

[!] Title: LayerSlider <= 6.2.0 - CSRF / Authenticated Stored XSS & SQL Injection
Reference: http://packetstormsecurity.com/files/125637/
Reference: https://secunia.com/advisories/57309/
[i] Fixed in: 5.2.0

[!] Title: LayerSlider <= 6.2.0 - CSRF / Authenticated Stored XSS & SQL Injection
Reference: https://wpvulndb.com/vulnerabilities/8822
Reference: http://wphutte.com/layer-slider-6-1-6-csrf-to-xss-to-sqli-with-poc/
Reference: https://support.kreaturamedia.com/docs/layersliderwp/documentation.html#release-log
[i] Fixed in: 6.2.1

[+] Name: advanced-recent-posts - v0.6.14
| Latest version: 0.6.14 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/
| Readme: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/

[+] Name: akismet
| Latest version: 4.0.3
| Location: http://law.uii.ac.id/wp-content/plugins/akismet/
| Readme: http://law.uii.ac.id/wp-content/plugins/akismet/readme.txt

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8215
Reference: http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/
Reference: https://blog.sucuri.net/2015/10/security-

Reference: https://wpvulndb.com/vulnerabilities/8822 Reference: http://wphutte.com/layer-slider-6-1-6-csrf-to-xss-to-sqli-with-poc/ Reference: https://support.kreaturamedia.com/docs/layersliderwp/documentation.html#release-log [i] Fixed in: 6.2.1 [+] Name: advanced-recent-posts - v0.6.14 | Latest version: 0.6.14 (up to date) | Location: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/ | Readme: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/readme.txt [!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/advanced-recent-posts/ [+] Name: akismet | Latest version: 4.0 | Location: http://law.uii.ac.id/wp-content/plugins/akismet/ | Readme: http://law.uii.ac.id/wp-content/plugins/akismet/readme.txt [!] We could not determine a version so all vulnerabilities are printed out [!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS) Reference: https://wpvulndb.com/vulnerabilities/8215 Reference: http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/ Reference: https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html [i] Fixed in: 3.1.5 [+] Name: all-in-one-wp-security-and-firewall | Latest version: 4.2.9 | Location: http://law.uii.ac.id/wp-content/plugins/all-in-one-wp-security-and-firewall/	advisory-stored-xss-in-akismet-wordpress-plugin.html [i] Fixed in: 3.1.5 [+] Name: all-in-one-wp-security-and-firewall | Latest version: 4.3.2 | Location: http://law.uii.ac.id/wp-content/plugins/all-in-one-wp-security-and-firewall/ | Readme: http://law.uii.ac.id/wp-content/plugins/all-in-one-wp-security-and-firewall/readme.txt [!] We could not determine a version so all vulnerabilities are printed out [!] Title: All In One WP Security plugin 3.8.2 - 2xSQL Injections Reference: https://wpvulndb.com/vulnerabilities/7600 Reference: http://www.securityfocus.com/archive/1/533519 Reference: https://www.htbridge.com/advisory/HTB23231 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6242 [i] Fixed in: 3.8.3 [!] Title: All In One WP Security & Firewall <= 3.8.7 - SQL Injection Reference: https://wpvulndb.com/vulnerabilities/7834 Reference: http://jvn.jp/en/jp/JVN30832515/index.html Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0894 [i] Fixed in: 3.8.8 [!] Title: All In One WP Security & Firewall <= 3.8.9 - CSRF Reference: https://wpvulndb.com/vulnerabilities/7835 Reference: http://jvn.jp/en/jp/JVN87204433/index.html Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0895 [i] Fixed in: 3.9.0

| Readme: http://law.uii.ac.id/wp-content/plugins/all-in-one-wp-security-and-firewall/readme.txt

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: All In One WP Security plugin 3.8.2 - 2xSQL Injections
Reference: https://wpvulndb.com/vulnerabilities/7600
Reference: http://www.securityfocus.com/archive/1/533519
Reference: https://www.htbridge.com/advisory/HTB23231
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6242
[i] Fixed in: 3.8.3

[!] Title: All In One WP Security & Firewall <= 3.8.7 - SQL Injection
Reference: https://wpvulndb.com/vulnerabilities/7834
Reference: http://jvn.jp/en/jp/JVN30832515/index.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0894
[i] Fixed in: 3.8.8

[!] Title: All In One WP Security & Firewall <= 3.8.9 - CSRF
Reference: https://wpvulndb.com/vulnerabilities/7835
Reference: http://jvn.jp/en/jp/JVN87204433/index.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0895
[i] Fixed in: 3.9.0

[!] Title: All In One WP Security & Firewall <= 3.9.0 - Blind SQL Injection
Reference: https://wpvulndb.com/vulnerabilities/7886
Reference: http://www.homelab.it/index.php/2015/04/07/wordpress-all-in-one-wp-security-sql-injection-vulnerability/

[!] Title: All In One WP Security & Firewall <= 3.9.0 - Blind SQL Injection
Reference: https://wpvulndb.com/vulnerabilities/7886
Reference: http://www.homelab.it/index.php/2015/04/07/wordpress-all-in-one-wp-security-sql-injection-vulnerability/
Reference: http://packetstormsecurity.com/files/131317/
Reference: https://www.exploit-db.com/exploits/36671/
[i] Fixed in: 3.9.1

[!] Title: All In One WP Security & Firewall <= 3.9.7 - Unauthenticated Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8245
Reference: http://cinu.pl/research/wp-plugins/mail_38c27c99f98a7b62cd8c7d4b6866a23d.html
Reference: http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html
[i] Fixed in: 3.9.8

[!] Title: All In One WP Security & Firewall <= 4.1.2 - Multiple vulnerabilities in login CAPTCHA
Reference: https://wpvulndb.com/vulnerabilities/8573
Reference: https://sumofpwn.nl/advisory/2016/multiple_vulnerabilities_in_all_in_one_wp_security___firewall_plugin_login_captcha.html
Reference: http://seclists.org/fulldisclosure/2016/Jul/88
[i] Fixed in: 4.1.3

[!] Title: All In One WP Security & Firewall 4.1.4-4.1.9 - Authenticated Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8665
Reference: https://sumofpwn.nl/advisory/2016/cross_site_scripting_in_all_in_one_wp_security___firewall_wordpress_plugin.html

Reference: http://packetstormsecurity.com/files/131317/ Reference: https://www.exploit-db.com/exploits/36671/ [i] Fixed in: 3.9.1 [!] Title: All In One WP Security & Firewall <= 3.9.7 - Unauthenticated Cross-Site Scripting (XSS) Reference: https://wpvulndb.com/vulnerabilities/8245 Reference: http://cinu.pl/research/wp-plugins/mail_38c27c99f98a7b62cd8c7d4b6866a23d.html Reference: http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html [i] Fixed in: 3.9.8 [!] Title: All In One WP Security & Firewall <= 4.1.2 - Multiple vulnerabilities in login CAPTCHA Reference: https://wpvulndb.com/vulnerabilities/8573 Reference: https://sumofpwn.nl/advisory/2016/multiple_vulnerabilities_in_all_in_one_wp_security___firewall_plugin_login_captcha.html Reference: http://seclists.org/fulldisclosure/2016/Jul/88 [i] Fixed in: 4.1.3 [!] Title: All In One WP Security & Firewall 4.1.4-4.1.9 - Authenticated Cross-Site Scripting (XSS) Reference: https://wpvulndb.com/vulnerabilities/8665 Reference: https://sumofpwn.nl/advisory/2016/cross_site_scripting_in_all_in_one_wp_security___firewall_wordpress_plugin.html Reference: http://seclists.org/fulldisclosure/2016/Nov/79 [i] Fixed in: 4.2.0 [!] Title: All In One WP Security & Firewall <= 4.2.1 - Cross-Site Scripting (XSS) Reference: https://wpvulndb.com/vulnerabilities/8696	Reference: http://seclists.org/fulldisclosure/2016/Nov/79 [i] Fixed in: 4.2.0 [!] Title: All In One WP Security & Firewall <= 4.2.1 - Cross-Site Scripting (XSS) Reference: https://wpvulndb.com/vulnerabilities/8696 Reference: https://plugins.trac.wordpress.org/changeset/1534803/all-in-one-wp-security-and-firewall Reference: https://blog.ripstech.com/2016/the-state-of-wordpress-security/ [i] Fixed in: 4.2.2 [+] Name: broken-link-checker | Latest version: 1.11.5 | Location: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/ | Readme: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/readme.txt [!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/ [!] We could not determine a version so all vulnerabilities are printed out [!] Title: Broken Link Checker 1.9.1 - Bulk Action Form URL H&ling XSS Reference: https://wpvulndb.com/vulnerabilities/7046 Reference: https://secunia.com/advisories/56053/ [i] Fixed in: 1.9.2 [!] Title: Broken Link Checker 1.9.1 - Sort Direction Query Argument H&ling XSS Reference: https://wpvulndb.com/vulnerabilities/7047 Reference: https://secunia.com/advisories/56053/ [i] Fixed in: 1.9.2 [!] Title: Broken Link Checker 1.10.1 - Authenticated Stored XSS

Reference: https://plugins.trac.wordpress.org/changeset/1534803/all-in-one-wp-security-and-firewall
Reference: https://blog.ripstech.com/2016/the-state-of-wordpress-security/
[i] Fixed in: 4.2.2

[+] Name: any-mobile-theme-switcher
| Latest version: 2.1
| Location: http://law.uii.ac.id/wp-content/plugins/any-mobile-theme-switcher/

[+] Name: broken-link-checker
| Latest version: 1.11.5
| Location: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/
| Readme: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/broken-link-checker/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Broken Link Checker 1.9.1 - Bulk Action Form URL H&ling XSS
Reference: https://wpvulndb.com/vulnerabilities/7046
Reference: https://secunia.com/advisories/56053/
[i] Fixed in: 1.9.2

[!] Title: Broken Link Checker 1.9.1 - Sort Direction Query Argument H&ling XSS
Reference: https://wpvulndb.com/vulnerabilities/7047
Reference: https://secunia.com/advisories/56053/
[i] Fixed in: 1.9.2

[!] Title: Broken Link Checker 1.10.1 - Authenticated Stored XSS
Reference: https://wpvulndb.com/vulnerabilities/7707
Reference: https://wordpress.org/plugins/broken-link-checker/changelog/
Reference: https://wpvulndb.com/vulnerabilities/7707
Reference: https://wordpress.org/plugins/broken-link-checker/changelog/
[i] Fixed in: 1.10.2

[!] Title: Broken Link Checker <= 1.10.5 - CSRF/XSS
Reference: https://wpvulndb.com/vulnerabilities/7926
Reference: https://blog.sucuri.net/2015/04/security-advisory-xss-vulnerability-affecting-multiple-wordpress-plugins.html
[i] Fixed in: 1.10.6

[!] Title: Broken Link Checker <= 1.10.8 - Unauthenticated Stored XSS
Reference: https://wpvulndb.com/vulnerabilities/8064
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5057
[i] Fixed in: 1.10.9

[+] Name: contact-form-7
| Latest version: 5.0.1
| Location: http://law.uii.ac.id/wp-content/plugins/contact-form-7/
| Readme: http://law.uii.ac.id/wp-content/plugins/contact-form-7/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/contact-form-7/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Contact Form 7 <= 3.7.1 - Security Bypass
Reference: https://wpvulndb.com/vulnerabilities/7020
Reference: http://www.securityfocus.com/bid/66381/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2265
[i] Fixed in: 3.7.2

[i] Fixed in: 1.10.2

[!] Title: Broken Link Checker <= 1.10.5 - CSRF/XSS
Reference: https://wpvulndb.com/vulnerabilities/7926
Reference: https://blog.sucuri.net/2015/04/security-advisory-xss-vulnerability-affecting-multiple-wordpress-plugins.html
[i] Fixed in: 1.10.6

[!] Title: Broken Link Checker <= 1.10.8 - Unauthenticated Stored XSS
Reference: https://wpvulndb.com/vulnerabilities/8064
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5057
[i] Fixed in: 1.10.9

[+] Name: contact-form-7
| Latest version: 4.9
| Location: http://law.uii.ac.id/wp-content/plugins/contact-form-7/
| Readme: http://law.uii.ac.id/wp-content/plugins/contact-form-7/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/contact-form-7/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Contact Form 7 <= 3.7.1 - Security Bypass
Reference: https://wpvulndb.com/vulnerabilities/7020
Reference: http://www.securityfocus.com/bid/66381/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2265
[i] Fixed in: 3.7.2

[!] Title: Contact Form 7 <= 3.5.2 - File Upload Remote Code Execution
Reference: https://wpvulndb.com/vulnerabilities/7022
Reference: http://packetstormsecurity.com/files/124154/
[i] Fixed in: 3.5.3

[!] Title: Contact Form 7 <= 3.5.2 - File Upload Remote Code Execution
Reference: https://wpvulndb.com/vulnerabilities/7022
Reference: http://packetstormsecurity.com/files/124154/
[i] Fixed in: 3.5.3

[+] Name: google-analytics-dashboard-for-wp - v5.3.2
| Latest version: 5.3.2 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/
| Readme: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/

[+] Name: google-sitemap-generator - v4.0.9
| Latest version: 4.0.9 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/google-sitemap-generator/
| Readme: http://law.uii.ac.id/wp-content/plugins/google-sitemap-generator/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/google-sitemap-generator/

[+] Name: loco-translate - v2.1.2
| Location: http://law.uii.ac.id/wp-content/plugins/loco-translate/
| Readme: http://law.uii.ac.id/wp-content/plugins/loco-translate/readme.txt
[!] The version is out of date, the latest version is 2.1.3
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/loco-translate/

[+] Name: meteor-slides - v1.5.6
| Latest version: 1.5.6 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/meteor-slides/

[+] Name: cs-framework
 | Location: http://law.uii.ac.id/wp-content/plugins/cs-framework/
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/cs-framework/

[+] Name: easy-social-share-buttons
 | Latest version: 1.4.2
 | Location: http://law.uii.ac.id/wp-content/plugins/easy-social-share-buttons/

[+] Name: google-analytics-dashboard-for-wp - v5.1.2
 | Latest version: 5.1.2 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/
 | Readme: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/google-analytics-dashboard-for-wp/

[+] Name: google-calendar-agenda - v1.2
 | Latest version: 1.2 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/google-calendar-agenda/
 | Readme: http://law.uii.ac.id/wp-content/plugins/google-calendar-agenda/readme.txt

[+] Name: js_composer
 | Location: http://law.uii.ac.id/wp-content/plugins/js_composer/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Visual Composer <= 4.7.3 - Multiple Unspecified Cross-Site Scripting (XSS)
 Reference: https://wpvulndb.com/vulnerabilities/8208
 Reference: http://codecanyon.net/item/visual-composer-page-builder-for-wordpress/242431
 | Readme: http://law.uii.ac.id/wp-content/plugins/meteor-slides/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/meteor-slides/

[+] Name: recent-posts-widget-with-thumbnails - v6.1
 | Latest version: 6.1 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/recent-posts-widget-with-thumbnails/
 | Readme: http://law.uii.ac.id/wp-content/plugins/recent-posts-widget-with-thumbnails/README.txt

[+] Name: tablepress - v1.9
 | Latest version: 1.9 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/tablepress/
 | Readme: http://law.uii.ac.id/wp-content/plugins/tablepress/readme.txt

[+] Name: the-events-calendar - v4.6.13
 | Latest version: 4.6.13 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/the-events-calendar/
 | Readme: http://law.uii.ac.id/wp-content/plugins/the-events-calendar/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/the-events-calendar/

[+] Name: updraftplus - v1.14.5
 | Latest version: 1.14.5 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/updraftplus/
 | Readme: http://law.uii.ac.id/wp-content/plugins/updraftplus/readme.txt
 | Changelog: http://law.uii.ac.id/wp-content/plugins/updraftplus/changelog.txt

[+] Name: wordfence - v7.1.2
 | Latest version: 7.1.2 (up to date)
 | Location: http://law.uii.ac.id/wp-content/plugins/wordfence/

Reference: https://forums.envato.com/t/visual-composer-security-vulnerability-fix/10494/7
[i] Fixed in: 4.7.4

[+] Name: loco-translate - v2.0.16
| Latest version: 2.0.16 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/loco-translate/
| Readme: http://law.uii.ac.id/wp-content/plugins/loco-translate/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/loco-translate/

[+] Name: meteor-slides - v1.5.6
| Latest version: 1.5.6 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/meteor-slides/
| Readme: http://law.uii.ac.id/wp-content/plugins/meteor-slides/readme.txt
[!] Directory listing is enabled: http://law.uii.ac.id/wp-content/plugins/meteor-slides/

[+] Name: recent-posts-widget-with-thumbnails - v5.1.2
| Latest version: 5.1.2 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/recent-posts-widget-with-thumbnails/
| Readme: http://law.uii.ac.id/wp-content/plugins/recent-posts-widget-with-thumbnails/README.txt

[+] Name: tablepress - v1.8.1
| Latest version: 1.8.1 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/tablepress/
| Readme: http://law.uii.ac.id/wp-content/plugins/tablepress/readme.txt

[+] Name: updraftplus - v1.13.11
| Latest version: 1.13.11 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/updraftplus/
| Readme: http://law.uii.ac.id/wp-content/plugins/updraftplus/readme.txt

| Readme: http://law.uii.ac.id/wp-content/plugins/wordfence/readme.txt

[+] Name: wordpress-seo - v7.2
| Latest version: 7.2 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/wordpress-seo/
| Readme: http://law.uii.ac.id/wp-content/plugins/wordpress-seo/readme.txt

[+] Name: wp-fastest-cache - v0.8.7.8
| Latest version: 0.8.7.8 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/wp-fastest-cache/
| Readme: http://law.uii.ac.id/wp-content/plugins/wp-fastest-cache/readme.txt

[+] Enumerating installed themes (only ones marked as popular) ...

Time: 00:06:10 <========================> (400 / 400) 100.00% Time: 00:06:10

[+] We found 1 themes:

[+] Name: enfold - v4.0.2
| Location: http://law.uii.ac.id/wp-content/themes/enfold/
| Style URL: http://law.uii.ac.id/wp-content/themes/enfold/style.css
| Theme Name: Enfold
| Theme URI: www.kriesi.at/themes/enfold/
| Description: A superflexible and responsive Business Theme by Kriesi -
 Update notificat...
| Author: Kriesi
| Author URI: http://www.kriesi.at

[!] Title: Enfold Theme <= 4.2 - Rewrite Portfolio Permalink Structure & Information Disclosure
Reference: https://wpvulndb.com/vulnerabilities/9018
Reference: https://kriesi.at/documentation/enfold/enfold-changelog/
[i] Fixed in: 4.2.1

| Changelog: http://law.uii.ac.id/wp-content/plugins/updraftplus/changelog.txt

[+] Name: woocommerce-social-media-share-buttons
| Latest version: 1.3.0
| Location: http://law.uii.ac.id/wp-content/plugins/woocommerce-social-media-share-buttons/

[+] Name: wordfence - v6.3.19
| Latest version: 6.3.19 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/wordfence/
| Readme: http://law.uii.ac.id/wp-content/plugins/wordfence/readme.txt

[+] Name: wordpress-seo - v5.5.1
| Location: http://law.uii.ac.id/wp-content/plugins/wordpress-seo/
| Readme: http://law.uii.ac.id/wp-content/plugins/wordpress-seo/readme.txt
[!] The version is out of date, the latest version is 5.6

[+] Name: wp-fastest-cache - v0.8.7.3
| Latest version: 0.8.7.3 (up to date)
| Location: http://law.uii.ac.id/wp-content/plugins/wp-fastest-cache/
| Readme: http://law.uii.ac.id/wp-content/plugins/wp-fastest-cache/readme.txt

[+] Enumerating installed themes (only ones marked as popular) ...

Time: 00:09:55 <==========> (400 / 400) 100.00% Time: 00:09:55

[+] We found 1 themes:

[+] Name: uoc-theme - v1.1
| Location: http://law.uii.ac.id/wp-content/themes/uoc-theme/
| Readme: http://law.uii.ac.id/wp-content/themes/uoc-theme/readme.txt
| Style URL: http://law.uii.ac.id/wp-content/themes/uoc-theme/style.css
| Theme Name: Uoc Theme

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Wed Apr 18 06:45:52 2018
[+] Requests Done: 2040
[+] Memory used: 162.277 MB
[+] Elapsed time: 00:33:56

| Theme URI: http://themeforest.net/user/chimpstudio | Description: UOCE (University of College Education) is elegant, customizable, easy, and clear WordPress theme.... | Author: Chimpstudio | Author URI: http://themeforest.net/user/chimpstudio [+] Enumerating usernames ... [+] We did not enumerate any usernames [+] Finished: Thu Oct 12 07:17:09 2017 [+] Requests Done: 2078 [+] Memory used: 151.832 MB [+] Elapsed time: 00:59:11	

Dpka.uii.ac.id	
Hasil pertama	Hasi kedua
wpscan --url www.dpka.uii.ac.id --enumerate p,u,t _____ _____ __ _____ _____ \ \ / / __ \ / ____| \ \ /\ / /| |__) | (___ ___ __ _ _ __ ® \ \/ \/ / | ___/ ___ \ / __|/ _` | '_ \ \ /\ / | | ____) | (__| (_| | | | \/ \/ |_| |_____/ ___|__,_|_| |_| WordPress Security Scanner by the WPScan Team Version 2.9.2 Sponsored by Sucuri - https://sucuri.net @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_ _____ _____ [i] The remote host tried to redirect to: http://dpka.uii.ac.id/ [?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y [+] URL: http://dpka.uii.ac.id/ [+] Started: Thu Oct 12 19:17:34 2017	root@kali:~# wpscan --url www.dpka.uii.ac.id --enumerate p,u,t _____ _____ __ _____ _____ \ \ / / __ \ / ____| \ \ /\ / /| |__) | (___ ___ __ _ _ __ ® \ \/ \/ / | ___/ ___ \ / __|/ _` | '_ \ \ /\ / | | ____) | (__| (_| | | | \/ \/ |_| |_____/ ___|__,_|_| |_| WordPress Security Scanner by the WPScan Team Version 2.9.2 Sponsored by Sucuri - https://sucuri.net @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_ _____ _____ [i] The remote host tried to redirect to: http://dpka.uii.ac.id/ [?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y [+] URL: http://dpka.uii.ac.id/ [+] Started: Wed Apr 18 07:27:53 2018

[!] The WordPress 'http://dpka.uii.ac.id/readme.html' file exists exposing a version number [+] Interesting header: LINK: <http://dpka.uii.ac.id/wp-json/>; rel="https://api.w.org/", <http://dpka.uii.ac.id/>; rel=shortlink [+] Interesting header: SERVER: nginx [+] Interesting header: X-CONTENT-TYPE-OPTIONS: nosniff [+] Interesting header: X-NGINX-CACHE-STATUS: MISS [+] Interesting header: X-SERVER-POWERED-BY: Engintron [+] Interesting header: X-XSS-PROTECTION: 1; mode=block [+] XML-RPC Interface available under: http://dpka.uii.ac.id/xmlrpc.php [!] Upload directory has directory listing enabled: http://dpka.uii.ac.id/wp-content/uploads/ [!] Includes directory has directory listing enabled: http://dpka.uii.ac.id/wp-includes/ [+] WordPress version 4.4.11 (Released on 2017-09-19) identified from advanced fingerprinting, meta generator, readme, links opml, stylesheets numbers [!] 1 vulnerability identified from the version number [!] Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset Reference: https://wpvulndb.com/vulnerabilities/8807 Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html Reference: https://core.trac.wordpress.org/ticket/25239 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295 [+] WordPress theme in use: university - v2.0.10	[!] The WordPress 'http://dpka.uii.ac.id/readme.html' file exists exposing a version number [+] Interesting header: LINK: <http://dpka.uii.ac.id/wp-json/>; rel="https://api.w.org/", <http://dpka.uii.ac.id/>; rel=shortlink [+] Interesting header: SERVER: Apache [+] XML-RPC Interface available under: http://dpka.uii.ac.id/xmlrpc.php [!] Upload directory has directory listing enabled: http://dpka.uii.ac.id/wp-content/uploads/ [!] Includes directory has directory listing enabled: http://dpka.uii.ac.id/wp-includes/ [+] WordPress version 4.4.15 (Released on 2018-04-03) identified from meta generator, links opml [+] WordPress theme in use: university - v2.0.10 [+] Name: university - v2.0.10 | Latest version: 1.3 (up to date) | Location: http://dpka.uii.ac.id/wp-content/themes/university/ | Readme: http://dpka.uii.ac.id/wp-content/themes/university/readme.txt | Style URL: http://dpka.uii.ac.id/wp-content/themes/university/style.css | Theme Name: university | Theme URI: http://cactusthemes.com/ | Description: A multi-purposes theme, suitable for colleagues, training centres, event organizers, business, sh... | Author: CactusThemes | Author URI: http://themeforest.net/user/cactusthemes [+] Enumerating installed plugins (only ones marked as popular) ... Time: 00:03:43 <=======================> (1496 / 1496) 100.00% Time: 00:03:43 [+] We found 5 plugins: [+] Name: akismet | Latest version: 4.0.3

[+] Name: university - v2.0.10
 | Latest version: 1.2 (up to date)
 | Location: http://dpka.uii.ac.id/wp-content/themes/university/
 | Readme: http://dpka.uii.ac.id/wp-content/themes/university/readme.txt
 | Style URL: http://dpka.uii.ac.id/wp-content/themes/university/style.css
 | Theme Name: university
 | Theme URI: http://cactusthemes.com/
 | Description: A multi-purposes theme, suitable for colleagues, training centres, event organizers, business, sh...
 | Author: CactusThemes
 | Author URI: http://themeforest.net/user/cactusthemes

[+] Enumerating installed plugins (only ones marked as popular) ...

 Time: 00:05:49 <=======================> (1500 / 1500) 100.00% Time: 00:05:49

[+] We found 5 plugins:

[+] Name: akismet
 | Latest version: 4.0
 | Location: http://dpka.uii.ac.id/wp-content/plugins/akismet/
 | Readme: http://dpka.uii.ac.id/wp-content/plugins/akismet/readme.txt

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS)
 Reference: https://wpvulndb.com/vulnerabilities/8215
 Reference: http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/
 Reference: https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html
[i] Fixed in: 3.1.5

 | Location: http://dpka.uii.ac.id/wp-content/plugins/akismet/
 | Readme: http://dpka.uii.ac.id/wp-content/plugins/akismet/readme.txt

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scripting (XSS)
 Reference: https://wpvulndb.com/vulnerabilities/8215
 Reference: http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/
 Reference: https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html
[i] Fixed in: 3.1.5

[+] Name: js_composer
 | Location: http://dpka.uii.ac.id/wp-content/plugins/js_composer/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Visual Composer <= 4.7.3 - Multiple Unspecified Cross-Site Scripting (XSS)
 Reference: https://wpvulndb.com/vulnerabilities/8208
 Reference: http://codecanyon.net/item/visual-composer-page-builder-for-wordpress/242431
 Reference: https://forums.envato.com/t/visual-composer-security-vulnerability-fix/10494/7
[i] Fixed in: 4.7.4

[+] Name: revslider
 | Location: http://dpka.uii.ac.id/wp-content/plugins/revslider/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: WordPress Slider Revolution Local File Disclosure

[+] Name: js_composer
 | Location: http://dpka.uii.ac.id/wp-content/plugins/js_composer/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Visual Composer <= 4.7.3 - Multiple Unspecified Cross-Site Scripting (XSS)
 Reference: https://wpvulndb.com/vulnerabilities/8208
 Reference: http://codecanyon.net/item/visual-composer-page-builder-for-wordpress/242431
 Reference: https://forums.envato.com/t/visual-composer-security-vulnerability-fix/10494/7
[i] Fixed in: 4.7.4

[+] Name: revslider
 | Location: http://dpka.uii.ac.id/wp-content/plugins/revslider/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: WordPress Slider Revolution Local File Disclosure
 Reference: https://wpvulndb.com/vulnerabilities/7540
 Reference: http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html
 Reference: http://packetstormsecurity.com/files/129761/
 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1579
 Reference: https://www.exploit-db.com/exploits/34511/
 Reference: https://www.exploit-db.com/exploits/36039/
[i] Fixed in: 4.1.5

[!] Title: WordPress Slider Revolution Shell Upload
 Reference: https://wpvulndb.com/vulnerabilities/7954
 Reference: https://wpvulndb.com/vulnerabilities/7540
 Reference: http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html
 Reference: http://packetstormsecurity.com/files/129761/
 Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1579
 Reference: https://www.exploit-db.com/exploits/34511/
 Reference: https://www.exploit-db.com/exploits/36039/
[i] Fixed in: 4.1.5

[!] Title: WordPress Slider Revolution Shell Upload
 Reference: https://wpvulndb.com/vulnerabilities/7954
 Reference: https://whatisgon.wordpress.com/2014/11/30/another-revslider-vulnerability/
 Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_revslider_upload_execute
 Reference: https://www.exploit-db.com/exploits/35385/
[i] Fixed in: 3.0.96

[+] Name: u-event
 | Location: http://dpka.uii.ac.id/wp-content/plugins/u-event/
[!] Directory listing is enabled: http://dpka.uii.ac.id/wp-content/plugins/u-event/

[+] Name: u-shortcodes
 | Location: http://dpka.uii.ac.id/wp-content/plugins/u-shortcodes/
[!] Directory listing is enabled: http://dpka.uii.ac.id/wp-content/plugins/u-shortcodes/

[+] Enumerating installed themes (only ones marked as popular) ...

```
   Reference:
https://whatisgon.wordpress.com/2014/11/30/another-revslider-vulnerability/
   Reference:
https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_revslider_upload_execute
   Reference: https://www.exploit-db.com/exploits/35385/
[i] Fixed in: 3.0.96

[+] Name: u-event
 |  Location: http://dpka.uii.ac.id/wp-content/plugins/u-event/
[!] Directory listing is enabled: http://dpka.uii.ac.id/wp-content/plugins/u-event/

[+] Name: u-shortcodes
 |  Location: http://dpka.uii.ac.id/wp-content/plugins/u-shortcodes/
[!] Directory listing is enabled: http://dpka.uii.ac.id/wp-content/plugins/u-shortcodes/

[+] Enumerating installed themes (only ones marked as popular) ...

  Time: 00:01:54 <=========================> (400 / 400) 100.00% Time: 00:01:54

[+] We found 1 themes:

[+] Name: university - v2.0.10
 |  Latest version: 1.2 (up to date)
 |  Location: http://dpka.uii.ac.id/wp-content/themes/university/
 |  Readme: http://dpka.uii.ac.id/wp-content/themes/university/readme.txt
 |  Style URL: http://dpka.uii.ac.id/wp-content/themes/university/style.css
 |  Theme Name: university
 |  Theme URI: http://cactusthemes.com/
 |  Description: A multi-purposes theme, suitable for colleagues, training centres, event organizers, business, sh...
 |  Author: CactusThemes
  Time: 00:01:00 <=========================> (400 / 400) 100.00% Time: 00:01:00

[+] We found 1 themes:

[+] Name: university - v2.0.10
 |  Latest version: 1.3 (up to date)
 |  Location: http://dpka.uii.ac.id/wp-content/themes/university/
 |  Readme: http://dpka.uii.ac.id/wp-content/themes/university/readme.txt
 |  Style URL: http://dpka.uii.ac.id/wp-content/themes/university/style.css
 |  Theme Name: university
 |  Theme URI: http://cactusthemes.com/
 |  Description: A multi-purposes theme, suitable for colleagues, training centres, event organizers, business, sh...
 |  Author: CactusThemes
 |  Author URI: http://themeforest.net/user/cactusthemes

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:
   +----+-------+-------+
   | Id | Login | Name  |
   +----+-------+-------+
   | 1  | admin | admin |
   +----+-------+-------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Wed Apr 18 07:34:24 2018
[+] Requests Done: 2319
[+] Memory used: 201.434 MB
[+] Elapsed time: 00:06:30
```

| Author URI: http://themeforest.net/user/cactusthemes [+] Enumerating usernames ... [+] Identified the following 1 user/s: +----+-------+-------+ | Id | Login | Name | +----+-------+-------+ | 1 | admin | admin | +----+-------+-------+ [!] Default first WordPress username 'admin' is still used [+] Finished: Thu Oct 12 19:25:54 2017 [+] Requests Done: 2002 [+] Memory used: 157.781 MB [+] Elapsed time: 00:08:20	

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	3
Low	3
Informational	0

Alert Detail

High (Medium)	Path Traversal
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to

	reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.

URL	http://bpm.uii.ac.id/wp-login.php?action=lostpassword
Method	POST
Parameter	redirect_to
Attack	/wp-login.php
Instances	1
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use a whitelist of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not

	decode the same input twice. Such errors could be used to bypass whitelist schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	http://projects.webappsec.org/Path-Traversal http://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Source ID	1
High (Medium)	**Remote OS Command Injection**
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.

URL	http://bpm.uii.ac.id/news/723/?query=query%3Bstart-sleep+-s+15+%23
Method	GET
Parameter	query
Attack	query;start-sleep -s 15 #
URL	http://bpm.uii.ac.id/news/ami-kinerja-akademik-sebagai-upaya-menjamin-mutu-pendidikan-di-uii/?query=query%26timeout+%2FT+15
Method	GET
Parameter	query
Attack	query&timeout /T 15
Instances	2
Solution	If at all possible, use library calls rather than external processes to recreate the desired functionality. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field. Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error. If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters

	that do not pass an extremely strict whitelist (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection. If the program to be executed allows arguments to be specified within an input file or from standard input, then consider using that mode to pass arguments instead of the command line. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the system() function accepts a string that contains the entire command to be executed, whereas execl(), execve(), and others require an array of strings, one for each argument. In Windows, CreateProcess() only accepts one command at a time. In Perl, if system() is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." When constructing OS command strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will

	appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://www.owasp.org/index.php/Command_Injection
CWE Id	78
WASC Id	31
Source ID	1
Medium (Medium)	**X-Frame-Options Header Not Set**
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

URL	http://bpm.uii.ac.id/news/uii-sosialisasikan-kebijakan-sistem-penjaminan-mutu-2016/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/artikel/mercy-of-god-sebuah-refleksi-penjaminan-mutu-uii/
Method	GET
Parameter	X-Frame-Options

URL	http://bpm.uii.ac.id/news/materi-pelatihan-pengukuran-sasaran-mutu-bagi-kepala-divisi-di-lingkungan-uii/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/profil-bpm/tujuan-dan-peranan/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/bpm-uii-terima-studi-banding-fakultas-ekonomi-universitas-tujuh-belas-agustus-semarang/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/materi-pelatihan-pengukuran-sasaran-mutu-bagi-kepala-divisi-di-lingkungan-uii/embed/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/category/news/page/6/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/bpm-uii-menyelenggarakan-pelatihan-sistem-penjaminan-mutu-untuk-stie-yppi-rembang/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/page/4/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/uii-raih-peringkat-emas-sni-award-2017/
Method	GET

Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/agenda/on-site-evaluation-sni-award-2017/embed/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/agenda/perguruan-tinggi-dituntut-wujudkan-budaya-mutu/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/uii-pertahankan-sertifikat-international-organization-for-standarization-90012008/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/uii-selenggarakan-rapat-tinjauan-manajemen-sistem-penjaminan-mutu-universitas-rtm-spmu-hasil-monitoring-dan-evaluasi-semester-ganjil-20152016/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/agenda/agenda-bpm-uii-2-november-2016-pelatihan-sasaran-mutu-bagi-kepala-divisi/embed/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/category/news/page/7/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/page/5/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/profil-bpm/tujuan-dan-peranan/embed/

Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/news/bpm-uii-terima-studi-banding-universitas-muhammadiyah-sidoarjo/
Method	GET
Parameter	X-Frame-Options
URL	http://bpm.uii.ac.id/agenda/agenda-bpm-uii-7-oktober-2016-induksi-smpi-bagi-pengendali-sistem-mutu-dan-auditor/
Method	GET
Parameter	X-Frame-Options
Instances	179
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3
Medium (Medium)	**Directory Browsing**
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which can be accessed to read sensitive information.

URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/LayerSlider/static/
Method	GET

Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/plugins/contact-form-7/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-includes/js/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-includes/css/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/tf-flexslider/assets/js/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/tf-flexslider/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/plugins/contact-form-7/includes/css/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/tf-flexslider/assets/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/plugins/revslider/rs-plugin/js/
Method	GET

Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/LayerSlider/static/css/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/plugins/contact-form-7/includes/js/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/css/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-includes/js/jquery/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/js/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/LayerSlider/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/
Method	GET

Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/plugins/contact-form-7/includes/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-content/themes/Avada/framework/plugins/LayerSlider/static/js/
Method	GET
Attack	Parent Directory
URL	http://bpm.uii.ac.id/wp-includes/
Method	GET
Attack	Parent Directory
Instances	21
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48
Source ID	1

Medium (Medium)	**Format String Error**
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.

URL	http://bpm.uii.ac.id/wp-content/themes/Avada?query=ZAP%25n%25s%0A

Method	GET
Parameter	query
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
Instances	1
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a /%s

Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1
Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.

URL	http://bpm.uii.ac.id/artikel/mercy-of-god-sebuah-refleksi-penjaminan-mutu-uii/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/uii-sosialisasikan-kebijakan-sistem-penjaminan-mutu-2016/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit

Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/profil-bpm/tujuan-dan-peranan/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/page/5/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/materi-pelatihan-pengukuran-sasaran-mutu-bagi-kepala-divisi-di-lingkungan-uii/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/bpm-uii-terima-studi-banding-fakultas-ekonomi-universitas-tujuh-belas-agustus-semarang/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/uii-selenggarakan-lokakarya-pengembangan-sistem-penjaminan-mutu-uisu/

Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/?page_id=117
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/dev/wp-content/uploads/2015/06/2015.05.13.induksi-sistem-penjaminan-mutu-300x200.jpg
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/dev/wp-content/uploads/2015/06/2013.07.24.-pelatihan-auditor-internal.jpg
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/news/bpm-uii-terima-kunjungan-studi-banding-universitas-mercu-buana-yogyakarta/
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en

Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/dev/wp-content/uploads/2015/06/2013.08.26.-pembukaan-ami-Faisol-Bachnas-300x200.jpg
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/download/kebijakan-spm-2016/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/category/news/page/6/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/category/news/page/2/
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/news/bpm-uii-menyelenggarakan-pelatihan-sistem-penjaminan-mutu-untuk-stie-yppi-rembang/

Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/uii-selenggarakan-ami-kinerja-unit-tahun-2016/
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/news/uii-raih-peringkat-emas-sni-award-2017/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>
URL	http://bpm.uii.ac.id/news/pemerintah-dorong-pts-memperbaiki-kualitas/
Method	GET
Parameter	http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en
Evidence	<script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false&language=en"></script>
URL	http://bpm.uii.ac.id/news/bpm-uii-terima-studi-banding-universitas-muhammadiyah-sidoarjo/
Method	GET
Parameter	//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
Evidence	<script type="text/javascript" src="//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit"></script>

Instances	314
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3
Low (Medium)	**Password Autocomplete in Browser**
Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.

URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	user_pass
Evidence	<input type="password" name="pwd" id="user_pass" class="input" value="" size="20" />
URL	http://bpm.uii.ac.id/wp-login.php
Method	POST
Parameter	user_pass
Evidence	<input type="password" name="pwd" id="user_pass" aria-describedby="login_error" class="input" value="" size="20" />
URL	http://bpm.uii.ac.id/wp-login.php
Method	GET
Parameter	user_pass
Evidence	<input type="password" name="pwd" id="user_pass" class="input" value="" size="20" />

Instances	3
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	http://www.w3schools.com/tags/att_input_autocomplete.asp https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx
CWE Id	525
WASC Id	15
Source ID	3
Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

URL	http://bpm.uii.ac.id/wp-login.php?action=lostpassword
Method	POST
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://bpm.uii.ac.id/wp-login.php
Method	POST
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpress_sec_2296ed40ff8e737cb8a8ef68270148d8
Evidence	Set-Cookie: wordpress_sec_2296ed40ff8e737cb8a8ef68270148d8

URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpressuser_2296ed40ff8e737cb8a8ef68270148d8
Evidence	Set-Cookie: wordpressuser_2296ed40ff8e737cb8a8ef68270148d8
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpress_logged_in_2296ed40ff8e737cb8a8ef68270148d8
Evidence	Set-Cookie: wordpress_logged_in_2296ed40ff8e737cb8a8ef68270148d8
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://bpm.uii.ac.id/wp-login.php
Method	GET
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://bpm.uii.ac.id/wp-login.php?action=lostpassword
Method	GET
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wp-settings-0

Evidence	Set-Cookie: wp-settings-0
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpresspass_2296ed40ff8e737cb8a8ef68270148d8
Evidence	Set-Cookie: wordpresspass_2296ed40ff8e737cb8a8ef68270148d8
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wp-settings-time-0
Evidence	Set-Cookie: wp-settings-time-0
URL	http://bpm.uii.ac.id/wp-login.php?reauth=1&redirect_to=http%3A%2F%2Fbpm.uii.ac.id%2Fwp-admin%2F
Method	GET
Parameter	wordpress_2296ed40ff8e737cb8a8ef68270148d8
Evidence	Set-Cookie: wordpress_2296ed40ff8e737cb8a8ef68270148d8
Instances	12
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

Port *scanning*

Law.uii.ac.id

```
root@kali:~# nmap -sS -sV law.uii.ac.id

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-25 00:15 WIB
Nmap scan report for law.uii.ac.id (103.220.113.20)
Host is up (0.030s latency).
rDNS record for 103.220.113.20: cpanel-node01.uii.ac.id
Not shown: 989 filtered ports
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        Pure-FTPd
22/tcp   open   ssh        OpenSSH 5.3 (protocol 2.0)
53/tcp   closed domain
80/tcp   open   http       Apache httpd
110/tcp  open   pop3       Dovecot pop3d
143/tcp  open   imap       Dovecot imapd
443/tcp  open   ssl/http   Apache httpd
587/tcp  open   smtp       Exim smtpd 4.89
993/tcp  open   ssl/imap   Dovecot imapd
995/tcp  open   ssl/pop3   Dovecot pop3d
8080/tcp closed http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.86 seconds
root@kali:~# nmap -sM -p21,22,80,110,143,443,587,993,995 103.220.113.20

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-25 00:17 WIB
Nmap scan report for cpanel-node01.uii.ac.id (103.220.113.20)
Host is up (0.0029s latency).
PORT    STATE         SERVICE
21/tcp  open|filtered ftp
22/tcp  open|filtered ssh
80/tcp  open|filtered http
110/tcp open|filtered pop3
143/tcp open|filtered imap
443/tcp open|filtered https
587/tcp open|filtered submission
993/tcp open|filtered imaps
995/tcp open|filtered pop3s

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

 nmap -sT -O law.uii.ac.id

Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-25 00:20 WIB
Nmap scan report for law.uii.ac.id (103.220.113.20)
Host is up (0.026s latency).
```

```
rDNS record for 103.220.113.20: cpanel-node01.uii.ac.id
Not shown: 986 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
53/tcp   closed domain
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
465/tcp  open   smtps
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
2002/tcp closed globe
8080/tcp closed http-proxy
8443/tcp closed https-alt
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (92%), WatchGuard Fireware 11.X (92%), Synology
DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1
cpe:/o:linux:linux_kernel:4.4
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 2.6.39 (92%),
WatchGuard Fireware 11.8 (92%), Synology DiskStation Manager 5.1 (91%), Linux 3.4 (91%), Linux 3.1
- 3.2 (90%), Linux 3.10 (89%), Linux 2.6.32 - 2.6.39 (89%), Linux 2.6.32 - 3.0 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.37 seconds
```

```
masscan 103.220.113.20 -p 0-10000

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-10-11 18:53:08 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [10001 ports/host]
Discovered open port 2078/tcp on 103.220.113.20
Discovered open port 587/tcp on 103.220.113.20
Discovered open port 21/tcp on 103.220.113.20
Discovered open port 2077/tcp on 103.220.113.20
Discovered open port 8080/tcp on 103.220.113.20
Discovered open port 443/tcp on 103.220.113.20
Discovered open port 2096/tcp on 103.220.113.20
Discovered open port 2082/tcp on 103.220.113.20
Discovered open port 2083/tcp on 103.220.113.20
Discovered open port 110/tcp on 103.220.113.20
```

```
Discovered open port 80/tcp on 103.220.113.20
Discovered open port 465/tcp on 103.220.113.20
Discovered open port 6556/tcp on 103.220.113.20
Discovered open port 2080/tcp on 103.220.113.20
Discovered open port 2002/tcp on 103.220.113.20
Discovered open port 995/tcp on 103.220.113.20
Discovered open port 2087/tcp on 103.220.113.20
Discovered open port 2086/tcp on 103.220.113.20
Discovered open port 143/tcp on 103.220.113.20
```

```
nmap -sS 103.220.113.20

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-11 18:51 UTC
Nmap scan report for cpanel-node01.uii.ac.id (103.220.113.20)
Host is up (0.23s latency).
Not shown: 985 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
22/tcp   closed ssh
53/tcp   closed domain
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
465/tcp  open   smtps
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
2002/tcp open   globe
8080/tcp open   http-proxy
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 184.50 seconds
```

```
nmap -sV 103.220.113.20

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-11 18:52 UTC
Nmap scan report for cpanel-node01.uii.ac.id (103.220.113.20)
Host is up (0.13s latency).
Not shown: 985 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      Pure-FTPd
22/tcp   closed ssh
53/tcp   closed domain
80/tcp   open   http     nginx
110/tcp  open   pop3     Dovecot pop3d
143/tcp  open   imap     Dovecot imapd
```

```
443/tcp  open   ssl/http nginx
465/tcp  open   ssl/smtp Exim smtpd 4.89
587/tcp  open   smtp     Exim smtpd 4.89
993/tcp  open   ssl/imap Dovecot imapd
995/tcp  open   ssl/pop3 Dovecot pop3d
2002/tcp open   ssh      OpenSSH 5.3 (protocol 2.0)
8080/tcp open   http     Apache httpd
8443/tcp open   ssl/http Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.90 seconds
```

```
<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?><nmaprun
start="1507793379" profile_name="Intense scan, all TCP ports" xmloutputversion="1.04"
scanner="nmap" version="7.40" startstr="Thu Oct 12 07:29:39 2017" args="nmap -p 1-65535 -T4 -A -v
www.law.uii.ac.id"><scaninfo services="1-65535" protocol="tcp" numservices="65535"
type="syn"></scaninfo><verbose level="1"></verbose><debugging level="0"></debugging><output
type="interactive">
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 07:29 UTC
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating Ping Scan at 07:29
Scanning www.law.uii.ac.id (103.220.113.20) [4 ports]
Completed Ping Scan at 07:29, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:29
Completed Parallel DNS resolution of 1 host. at 07:29, 6.64s elapsed
Initiating SYN Stealth Scan at 07:29
Scanning www.law.uii.ac.id (103.220.113.20) [65535 ports]
Discovered open port 80/tcp on 103.220.113.20
Discovered open port 993/tcp on 103.220.113.20
Discovered open port 21/tcp on 103.220.113.20
Discovered open port 443/tcp on 103.220.113.20
Discovered open port 995/tcp on 103.220.113.20
Discovered open port 143/tcp on 103.220.113.20
Discovered open port 587/tcp on 103.220.113.20
Discovered open port 110/tcp on 103.220.113.20
Discovered open port 8080/tcp on 103.220.113.20
SYN Stealth Scan Timing: About 23.72% done; ETC: 07:31 (0:01:40 remaining)
SYN Stealth Scan Timing: About 60.24% done; ETC: 07:31 (0:00:40 remaining)
Discovered open port 2083/tcp on 103.220.113.20
Discovered open port 8443/tcp on 103.220.113.20
SYN Stealth Scan Timing: About 47.72% done; ETC: 07:32 (0:01:40 remaining)
SYN Stealth Scan Timing: About 65.31% done; ETC: 07:32 (0:01:04 remaining)
Completed SYN Stealth Scan at 07:32, 167.52s elapsed (65535 total ports)
```

```
Initiating Service scan at 07:32
Scanning 11 services on www.law.uii.ac.id (103.220.113.20)
Completed Service scan at 07:34, 133.49s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against www.law.uii.ac.id (103.220.113.20)
Retrying OS detection (try #2) against www.law.uii.ac.id (103.220.113.20)
Initiating Traceroute at 07:34
Completed Traceroute at 07:34, 2.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 07:34
Completed Parallel DNS resolution of 4 hosts. at 07:35, 13.00s elapsed
NSE: Script scanning 103.220.113.20.
Initiating NSE at 07:35
Completed NSE at 07:35, 35.49s elapsed
Initiating NSE at 07:35
Completed NSE at 07:35, 0.09s elapsed
Nmap scan report for www.law.uii.ac.id (103.220.113.20)
Host is up (0.013s latency).
rDNS record for 103.220.113.20: cpanel-node01.uii.ac.id
Not shown: 65522 filtered ports
PORT     STATE  SERVICE      VERSION
21/tcp   open   ftp          Pure-FTPd
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:13+00:00; -7h00m04s from scanner time.
22/tcp   closed ssh
53/tcp   closed domain
80/tcp   open   http         nginx
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-generator: Powered by LayerSlider 6.5.7 - Multi-Purpose, Responsive, Parallax, Mobile-Friendly
Slider Plugin for WordPress.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: nginx
| http-title: Home - Fakultas Hukum Program Studi Ilmu Hukum Pasca Sarjana H...
|_Requested resource was http://law.uii.ac.id/
110/tcp  open   pop3         Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE USER PIPELINING CAPA STLS UIDL TOP RESP-CODES
SASL(PLAIN LOGIN)
```

```
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:05+00:00; -7h00m04s from scanner time.
143/tcp  open   imap        Dovecot imapd
|_imap-capabilities: LITERAL+ capabilities ENABLE LOGIN-REFERRALS OK IDLE IMAP4rev1 STARTTLS
AUTH=PLAIN more AUTH=LOGINA0001 NAMESPACE post-login listed have ID Pre-login SASL-IR
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:10+00:00; -7h00m04s from scanner time.
443/tcp  open   ssl/http     nginx
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-generator: Powered by LayerSlider 6.5.7 - Multi-Purpose, Responsive, Parallax, Mobile-Friendly
Slider Plugin for WordPress.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: nginx
| http-title: Home - Fakultas Hukum Program Studi Ilmu Hukum Pasca Sarjana H...
|_Requested resource was https://law.uii.ac.id/
| ssl-cert: Subject: commonName=*.uii.ac.id
| Subject Alternative Name: DNS:*.uii.ac.id, DNS:uii.ac.id
| Issuer: commonName=RapidSSL SHA256 CA - G3/organizationName=GeoTrust
Inc./countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-01-17T17:00:14
| Not valid after:  2019-02-18T22:44:31
| MD5:   daa5 5041 f5b0 d7de d0af 640a 34e8 1d60
```

```
|_SHA-1: 05a0 b5a5 ee32 d896 d42e 6ef5 46a7 9943 8a85 a311
|_ssl-date: 2017-10-12T00:35:07+00:00; -7h00m04s from scanner time.
| tls-nextprotoneg:
|   h2
|_  http/1.1
587/tcp  open   smtp        Exim smtpd 4.89
| smtp-commands: cpanel-node01.uii.ac.id Hello www.law.uii.ac.id [180.246.144.76], SIZE 52428800,
8BITMIME, PIPELINING, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp  open   ssl/imap     Dovecot imapd
|_imap-capabilities: LITERAL+ capabilities ENABLE ID OK IDLE IMAP4rev1 SASL-IR AUTH=PLAIN more
AUTH=LOGINA0001 NAMESPACE post-login listed have LOGIN-REFERRALS Pre-login
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:04+00:00; -7h00m05s from scanner time.
995/tcp  open   ssl/pop3     Dovecot pop3d
|_pop3-capabilities: PIPELINING AUTH-RESP-CODE USER TOP CAPA SASL(PLAIN LOGIN) RESP-CODES
UIDL
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:15+00:00; -7h00m04s from scanner time.
2083/tcp open   ssl/radsec?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 401 Access Denied
|     Connection: close
|     Content-Type: text/html; charset="utf-8"
|     Date: Thu, 12 Oct 2017 00:32:58 GMT
|     Cache-Control: no-cache, no-store, must-revalidate, private
|     Pragma: no-cache
```

```
|     WWW-Authenticate: Basic realm="cPanel"
|     Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
secure
|     Set-Cookie: cpsession=%3alc2OpO9C9ZhML2p9%2c445aea997a0f9af5934cd6e65388a8f9;
HttpOnly; path=/; port=2083; secure
|     Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT;
path=/; port=2083; secure
|     Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=cpanel-node01.uii.ac.id;
expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
|     Set-Cookie: Horde=expired; HttpOnly; domain=.cpanel-node01.uii.ac.id; expires=Thu, 01-Jan-1970
00:00:01 GMT; path=/; port=2083; secure
|     Set-Cookie: horde_secret_key=expired; Ht
|   HTTPOptions:
|     HTTP/1.0 401 Access Denied
|     Connection: close
|     Content-Type: text/html; charset="utf-8"
|     Date: Thu, 12 Oct 2017 00:32:58 GMT
|     Cache-Control: no-cache, no-store, must-revalidate, private
|     Pragma: no-cache
|     WWW-Authenticate: Basic realm="cPanel"
|     Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
secure
|     Set-Cookie: cpsession=%3a7uzkMIfLGD8InpFa%2ce99cdcbe51f640d5b8a40caa4e5a8fb1;
HttpOnly; path=/; port=2083; secure
|     Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT;
path=/; port=2083; secure
|     Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=cpanel-node01.uii.ac.id;
expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
|     Set-Cookie: Horde=expired; HttpOnly; domain=.cpanel-node01.uii.ac.id; expires=Thu, 01-Jan-1970
00:00:01 GMT; path=/; port=2083; secure
|_    Set-Cookie: horde_secret_key=expired; Ht
| ssl-cert: Subject: commonName=cpanel-node01.uii.ac.id
| Subject Alternative Name: DNS:cpanel-node01.uii.ac.id, DNS:www.cpanel-node01.uii.ac.id
| Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel,
Inc./stateOrProvinceName=TX/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-12-13T00:00:00
| Not valid after:  2017-12-13T23:59:59
| MD5:   a6ae 6484 6c37 a0a4 c788 51ee 5b16 803f
|_SHA-1: 5100 130d d137 370a 1fe8 f968 8946 e378 bfd4 1a02
|_ssl-date: 2017-10-12T00:35:08+00:00; -7h00m04s from scanner time.
8080/tcp open   http         Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
```

```
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache
|_http-title: Did not follow redirect to http://law.uii.ac.id/
8443/tcp open   ssl/https-alt Apache
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://law.uii.ac.id/
| ssl-cert: Subject: commonName=*.uii.ac.id
| Subject Alternative Name: DNS:*.uii.ac.id, DNS:uii.ac.id
| Issuer: commonName=RapidSSL SHA256 CA - G3/organizationName=GeoTrust
Inc./countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-01-17T17:00:14
| Not valid after:  2019-02-18T22:44:31
| MD5:   daa5 5041 f5b0 d7de d0af 640a 34e8 1d60
|_SHA-1: 05a0 b5a5 ee32 d896 d42e 6ef5 46a7 9943 8a85 a311
|_ssl-date: 2017-10-12T00:35:11+00:00; -7h00m04s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port2083-TCP:V=7.40%T=SSL%I=7%D=10/12%Time=59DF1AAE%P=x86_64-pc-linux-g
SF:nu%r(GetRequest,4000,"HTTP/1\.0\x20401\x20Access\x20Denied\r\nConnectio
SF:n:\x20close\r\nContent-Type:\x20text/html;\x20charset=\"utf-8\"\r\nDate
SF::\x20Thu,\x2012\x20Oct\x202017\x2000:32:58\x20GMT\r\nCache-Control:\x20
SF:no-cache,\x20no-store,\x20must-revalidate,\x20private\r\nPragma:\x20no-
SF:cache\r\nWWW-Authenticate:\x20Basic\x20realm=\"cPanel\"\r\nSet-Cookie:\
SF:x20cprelogin=no;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x2000:00:0
SF:1\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20cpsessio
SF:n=%3alc2OpO9C9ZhML2p9%2c445aea997a0f9af5934cd6e65388a8f9;\x20HttpOnly;\
SF:x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20roundcube_sessid=e
SF:xpired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;
SF:\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20roundcube_sessaut
SF:h=expired;\x20HttpOnly;\x20domain=cpanel-node01\.uii\.ac\.id;\x20expire
SF:s=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20s
SF:ecure\r\nSet-Cookie:\x20Horde=expired;\x20HttpOnly;\x20domain=\.cpanel-
SF:node01\.uii\.ac\.id;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;
SF:\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20horde_secret_key=
SF:expired;\x20Ht")%r(HTTPOptions,4000,"HTTP/1\.0\x20401\x20Access\x20Deni
SF:ed\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charset=\"
SF:utf-8\"\r\nDate:\x20Thu,\x2012\x20Oct\x202017\x2000:32:58\x20GMT\r\nCac
SF:he-Control:\x20no-cache,\x20no-store,\x20must-revalidate,\x20private\r\
SF:nPragma:\x20no-cache\r\nWWW-Authenticate:\x20Basic\x20realm=\"cPanel\"\
```

```
SF:r\nSet-Cookie:\x20cprelogin=no;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-
SF:1970\x2000:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cook
SF:ie:\x20cpsession=%3a7uzkMIfLGD8InpFa%2ce99cdcbe51f640d5b8a40caa4e5a8fb1
SF:;\x20HttpOnly;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20rou
SF:ndcube_sessid=expired;\x20HttpOnly;\x20expires=Thu,\x2001-Jan-1970\x200
SF:0:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20ro
SF:undcube_sessauth=expired;\x20HttpOnly;\x20domain=cpanel-node01\.uii\.ac
SF:\.id;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20path=/;\x20
SF:port=2083;\x20secure\r\nSet-Cookie:\x20Horde=expired;\x20HttpOnly;\x20d
SF:omain=\.cpanel-node01\.uii\.ac\.id;\x20expires=Thu,\x2001-Jan-1970\x200
SF:0:00:01\x20GMT;\x20path=/;\x20port=2083;\x20secure\r\nSet-Cookie:\x20ho
SF:rde_secret_key=expired;\x20Ht");
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (92%), WatchGuard Fireware 11.X (92%), Synology
DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1
cpe:/o:linux:linux_kernel:4.0
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), WatchGuard Fireware 11.8
(92%), Synology DiskStation Manager 5.1 (91%), Linux 3.10 (91%), Linux 2.6.39 (91%), Linux 3.4 (91%),
Linux 3.1 - 3.2 (89%), Linux 2.6.32 - 2.6.39 (89%), Linux 4.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 14.466 days (since Wed Sep 27 20:24:07 2017)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

Host script results:
|_clock-skew: mean: -7h00m04s, deviation: 0s, median: -7h00m04s

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   6.35 ms 192.168.100.1
2   6.38 ms 180.246.144.1
3   8.51 ms 125.160.1.197
4   2.17 ms cpanel-node01.uii.ac.id (103.220.113.20)

NSE: Script Post-scanning.
Initiating NSE at 07:35
Completed NSE at 07:35, 0.00s elapsed
Initiating NSE at 07:35
Completed NSE at 07:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 363.60 seconds
        Raw packets sent: 262331 (11.547MB) | Rcvd: 181 (21.744KB)
```

```
</output><host comment=""><status state="up"></status><address addrtype="ipv4" vendor=""
addr="103.220.113.20"></address><hostnames><hostname type="user"
name="www.law.uii.ac.id"></hostname><hostname type="PTR" name="cpanel-
node01.uii.ac.id"></hostname></hostnames><ports><extraports count="65522"
state="filtered"></extraports><port protocol="tcp" portid="21"><state reason="syn-ack"
state="open" reason_ttl="54"></state><service product="Pure-FTPd" method="probed" conf="10"
name="ftp"></service></port><port protocol="tcp" portid="22"><state reason="reset"
state="closed" reason_ttl="54"></state><service method="table" conf="3"
name="ssh"></service></port><port protocol="tcp" portid="53"><state reason="reset"
state="closed" reason_ttl="54"></state><service method="table" conf="3"
name="domain"></service></port><port protocol="tcp" portid="80"><state reason="syn-ack"
state="open" reason_ttl="252"></state><service product="nginx" method="probed" conf="10"
name="http"></service></port><port protocol="tcp" portid="110"><state reason="syn-ack"
state="open" reason_ttl="54"></state><service product="Dovecot pop3d" method="probed"
conf="10" name="pop3"></service></port><port protocol="tcp" portid="143"><state reason="syn-
ack" state="open" reason_ttl="54"></state><service product="Dovecot imapd" method="probed"
conf="10" name="imap"></service></port><port protocol="tcp" portid="443"><state reason="syn-
ack" state="open" reason_ttl="54"></state><service product="nginx" method="probed" conf="10"
name="http"></service></port><port protocol="tcp" portid="587"><state reason="syn-ack"
state="open" reason_ttl="54"></state><service product="Exim smtpd" version="4.89"
method="probed" conf="10" name="smtp"></service></port><port protocol="tcp"
portid="993"><state reason="syn-ack" state="open" reason_ttl="54"></state><service
product="Dovecot imapd" method="probed" conf="10" name="imap"></service></port><port
protocol="tcp" portid="995"><state reason="syn-ack" state="open"
reason_ttl="54"></state><service product="Dovecot pop3d" method="probed" conf="10"
name="pop3"></service></port><port protocol="tcp" portid="2083"><state reason="syn-ack"
state="open" reason_ttl="54"></state><service method="table" conf="3"
name="radsec"></service></port><port protocol="tcp" portid="8080"><state reason="syn-ack"
state="open" reason_ttl="54"></state><service product="Apache httpd" method="probed"
conf="10" name="http"></service></port><port protocol="tcp" portid="8443"><state reason="syn-
ack" state="open" reason_ttl="54"></state><service product="Apache" method="probed" conf="10"
name="https-alt"></service></port></ports><os><portused state="open" portid="21"
proto="tcp"></portused><portused state="closed" portid="22" proto="tcp"></portused><osmatch
line="51466" name="Linux 2.6.32" accuracy="92"><osclass type="general purpose" osfamily="Linux"
vendor="Linux" osgen="2.6.X" accuracy="92"></osclass></osmatch><osmatch line="53915"
name="Linux 2.6.32 or 3.10" accuracy="92"><osclass type="general purpose" osfamily="Linux"
vendor="Linux" osgen="3.X" accuracy="92"></osclass></osmatch><osmatch line="98536"
name="WatchGuard Fireware 11.8" accuracy="92"><osclass type="firewall" osfamily="Fireware"
vendor="WatchGuard" osgen="11.X" accuracy="92"></osclass></osmatch><osmatch line="64359"
name="Synology DiskStation Manager 5.1" accuracy="91"><osclass type="storage-misc"
osfamily="DiskStation Manager" vendor="Synology" osgen="5.X"
accuracy="91"></osclass></osmatch><osmatch line="60110" name="Linux 3.10"
accuracy="91"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="3.X"
accuracy="91"></osclass></osmatch><osmatch line="55283" name="Linux 2.6.39"
accuracy="91"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="2.6.X"
accuracy="91"></osclass></osmatch><osmatch line="62192" name="Linux 3.4"
accuracy="91"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="3.X"
accuracy="91"></osclass></osmatch><osmatch line="59910" name="Linux 3.1 - 3.2"
```

accuracy="89"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="3.X"
accuracy="89"></osclass></osmatch><osmatch line="53496" name="Linux 2.6.32 - 2.6.39"
accuracy="89"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="2.6.X"
accuracy="89"></osclass></osmatch><osmatch line="63667" name="Linux 4.0"
accuracy="86"><osclass type="general purpose" osfamily="Linux" vendor="Linux" osgen="4.X"
accuracy="86"></osclass></osmatch></os><uptime lastboot="Wed Sep 27 20:24:07 2017"
seconds="1249895"></uptime><tcpsequence index="258"
values="8C80C0A7,B3F241F9,DD7B433,8E50FA09,E6CEC01B,9BD61181" difficulty="Good
luck!"></tcpsequence><ipidsequence values="0,0,0,0,0,0" class="All
zeros"></ipidsequence><tcptssequence
values="4A7F175A,4A7F17BE,4A7F1821,4A7F1886,4A7F18EA,4A7F194E"
class="1000HZ"></tcptssequence><trace port="80" proto="tcp"><hop rtt="6.35" host=""
ipaddr="192.168.100.1" ttl="1"></hop><hop rtt="6.38" host="" ipaddr="180.246.144.1"
ttl="2"></hop><hop rtt="8.51" host="" ipaddr="125.160.1.197" ttl="3"></hop><hop rtt="2.17"
host="cpanel-node01.uii.ac.id" ipaddr="103.220.113.20"
ttl="4"></hop></trace></host><runstats><finished timestr="Thu Oct 12 07:35:42 2017"
time="1507793742"></finished><hosts down="0" total="1" up="1"></hosts></runstats></nmaprun>